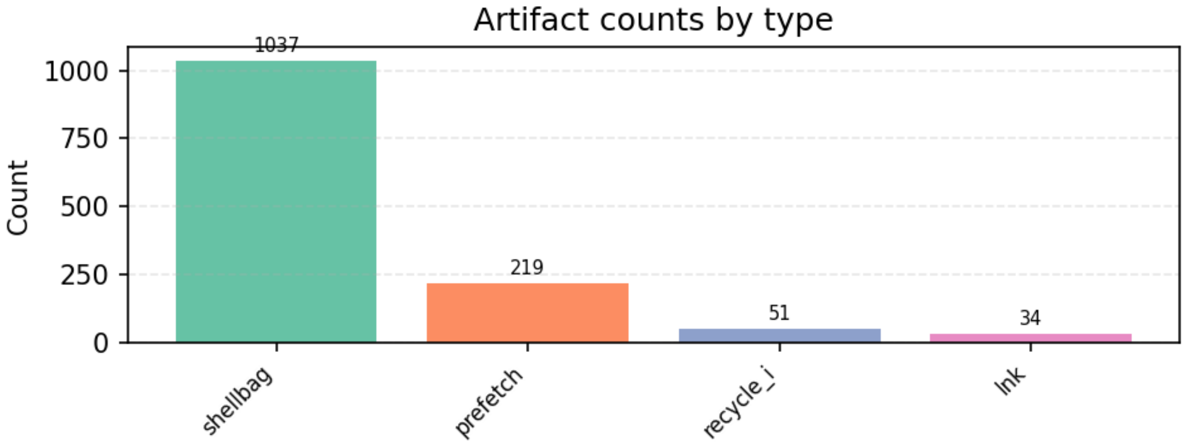
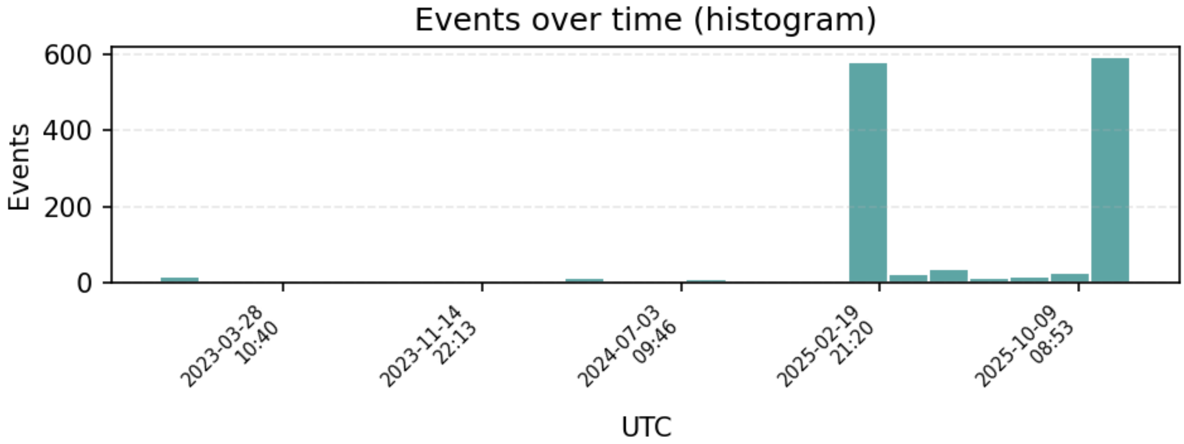
Correlation Report (Mukul)

Generated (UTC): 2025-12-09T21:33:32Z

Sessions: 262 Events: 1341



Artifact counts (by type)



Event distribution over time (histogram)

Session ID	Event Count	First Time	Last Time
1	12	2022-11-04T17:31:18.544000Z	2022-11-04T17:32:17.355000Z
2	1	2022-12-06T07:56:39.753000Z	2022-12-06T07:56:39.753000Z
3	4	2022-12-13T18:28:54.904980Z	2022-12-13T18:28:54.904980Z
4	1	2023-02-11T09:34:13.716330Z	2023-02-11T09:34:13.716330Z
5	1	2023-08-26T10:28:55.246372Z	2023-08-26T10:28:55.246372Z
6	1	2024-02-12T10:33:17.423267Z	2024-02-12T10:33:17.423267Z
7	1	2024-03-15T11:12:41.800748Z	2024-03-15T11:12:41.800748Z
8	12	2024-04-01T07:22:07.044074Z	2024-04-01T07:24:04.090008Z
9	2	2024-06-17T04:29:36.473032Z	2024-06-17T04:29:49.214784Z
10	2	2024-07-23T06:04:45.420000Z	2024-07-23T06:04:45.420000Z
11	4	2024-08-05T09:26:46.737000Z	2024-08-05T09:26:46.746000Z
12	2	2024-08-05T09:30:15.313000Z	2024-08-05T09:30:15.313000Z
13	1	2024-08-28T07:05:54.284000Z	2024-08-28T07:05:54.284000Z

Session ID	Event Count	First Time	Last Time
14	1	2024-08-29T10:33:38.299592Z	2024-08-29T10:33:38.299592Z
15	4	2024-08-30T05:35:59.687410Z	2024-08-30T05:36:28.123795Z
16	2	2024-12-12T16:00:58.080000Z	2024-12-12T16:00:58.080000Z
17	1	2025-01-09T07:47:51.608726Z	2025-01-09T07:47:51.608726Z
18	546	2025-01-14T16:02:27.688004Z	2025-01-14T16:02:30.094980Z
19	2	2025-01-14T22:51:17.446480Z	2025-01-14T22:51:39.837562Z
20	1	2025-01-19T08:56:23.057078Z	2025-01-19T08:56:23.057078Z
21	4	2025-01-19T09:32:20.929070Z	2025-01-19T09:32:56.410956Z
22	1	2025-01-19T10:09:18.307686Z	2025-01-19T10:09:18.307686Z
23	1	2025-01-19T10:27:22.859030Z	2025-01-19T10:27:22.859030Z
24	1	2025-01-19T10:36:57.441396Z	2025-01-19T10:36:57.441396Z
25	2	2025-01-19T10:45:29.479808Z	2025-01-19T10:45:38.427316Z
26	1	2025-01-19T10:49:01.176410Z	2025-01-19T10:49:01.176410Z
27	1	2025-01-19T11:01:49.483952Z	2025-01-19T11:01:49.483952Z
28	2	2025-01-19T11:12:55.255944Z	2025-01-19T11:13:04.150590Z
29	2	2025-01-19T11:54:12.558506Z	2025-01-19T11:54:12.558506Z
30	1	2025-01-19T12:11:01.196370Z	2025-01-19T12:11:01.196370Z
31	1	2025-01-19T16:49:43.751024Z	2025-01-19T16:49:43.751024Z
32	1	2025-01-23T05:34:17.828176Z	2025-01-23T05:34:17.828176Z
33	1	2025-01-23T06:53:56.914232Z	2025-01-23T06:53:56.914232Z
34	3	2025-01-31T07:08:04.128420Z	2025-01-31T07:08:51.026040Z
35	6	2025-01-31T09:54:44.239739Z	2025-01-31T09:56:07.715772Z
36	3	2025-02-06T07:16:42.122901Z	2025-02-06T07:16:42.122901Z
37	2	2025-02-10T18:29:49.084974Z	2025-02-10T18:29:49.084974Z
38	2	2025-03-09T07:49:06.395618Z	2025-03-09T07:49:17.543918Z
39	1	2025-03-09T07:57:48.500412Z	2025-03-09T07:57:48.500412Z
40	2	2025-03-09T08:05:18.005390Z	2025-03-09T08:05:18.005390Z
41	1	2025-03-09T08:10:07.792706Z	2025-03-09T08:10:07.792706Z
42	2	2025-03-09T08:12:16.579384Z	2025-03-09T08:12:16.580768Z
43	3	2025-03-12T09:31:09.916672Z	2025-03-12T09:31:09.916672Z
44	2	2025-03-12T09:33:27.843676Z	2025-03-12T09:33:27.843676Z
45	1	2025-03-25T13:30:05.718592Z	2025-03-25T13:30:05.718592Z
46	2	2025-04-15T07:55:47.212010Z	2025-04-15T07:56:45.402566Z
47	1	2025-04-15T08:27:19.793690Z	2025-04-15T08:27:19.793690Z
48	1	2025-04-16T07:08:48.015998Z	2025-04-16T07:08:48.015998Z
49	5	2025-04-16T07:18:02.534212Z	2025-04-16T07:18:33.551206Z
50	1	2025-04-28T21:35:49.345178Z	2025-04-28T21:35:49.345178Z
51	4	2025-05-04T21:46:44.712818Z	2025-05-04T21:46:52.309910Z
52	2	2025-05-04T22:00:08.537486Z	2025-05-04T22:00:08.537486Z

Session ID	Event Count	First Time	Last Time
53	2	2025-05-07T04:45:11.086402Z	2025-05-07T04:45:11.086402Z
54	1	2025-05-07T04:47:55.255084Z	2025-05-07T04:47:55.255084Z
55	1	2025-05-07T05:20:10.623300Z	2025-05-07T05:20:10.623300Z
56	2	2025-05-12T13:25:54.271126Z	2025-05-12T13:26:12.247356Z
57	1	2025-05-12T15:08:57.503496Z	2025-05-12T15:08:57.503496Z
58	2	2025-05-12T15:11:10.095556Z	2025-05-12T15:12:53.043882Z
59	1	2025-05-13T08:15:32.836056Z	2025-05-13T08:15:32.836056Z
60	1	2025-05-13T08:17:58.394160Z	2025-05-13T08:17:58.394160Z
61	1	2025-05-14T08:30:06.561202Z	2025-05-14T08:30:06.561202Z
62	1	2025-05-14T09:49:47.270186Z	2025-05-14T09:49:47.270186Z
63	3	2025-05-15T12:16:27.617120Z	2025-05-15T12:16:29.029204Z
64	1	2025-05-15T17:34:21.837690Z	2025-05-15T17:34:21.837690Z
65	1	2025-05-15T18:38:15.378844Z	2025-05-15T18:38:15.378844Z
66	1	2025-05-15T19:27:14.438152Z	2025-05-15T19:27:14.438152Z
67	2	2025-05-15T19:33:55.947992Z	2025-05-15T19:33:55.947992Z
68	6	2025-05-15T19:36:35.223120Z	2025-05-15T19:38:51.870024Z
69	1	2025-05-16T11:03:14.116000Z	2025-05-16T11:03:14.116000Z
70	2	2025-06-02T10:42:06.043000Z	2025-06-02T10:42:06.043000Z
71	1	2025-06-11T04:43:06.733076Z	2025-06-11T04:43:06.733076Z
72	2	2025-06-11T04:46:39.538492Z	2025-06-11T04:46:39.538492Z
73	2	2025-06-12T06:13:59.880170Z	2025-06-12T06:13:59.880170Z
74	3	2025-06-13T06:24:30.246674Z	2025-06-13T06:26:46.971938Z
75	1	2025-06-13T07:26:52.393516Z	2025-06-13T07:26:52.393516Z
76	3	2025-06-22T09:22:48.526526Z	2025-06-22T09:22:48.526526Z
77	1	2025-06-23T15:19:59.887568Z	2025-06-23T15:19:59.887568Z
78	1	2025-08-14T09:18:53.233248Z	2025-08-14T09:18:53.233248Z
79	1	2025-09-02T07:42:59.341038Z	2025-09-02T07:42:59.341038Z
80	1	2025-09-02T09:21:01.371860Z	2025-09-02T09:21:01.371860Z
81	3	2025-09-02T09:30:44.042565Z	2025-09-02T09:30:44.042565Z
82	3	2025-09-02T09:34:32.737498Z	2025-09-02T09:34:33.887454Z
83	3	2025-09-02T10:15:23.941691Z	2025-09-02T10:15:23.941691Z
84	4	2025-09-02T10:39:16.795132Z	2025-09-02T10:41:17.320704Z
85	2	2025-10-01T10:41:03.314266Z	2025-10-01T10:41:03.314266Z
86	2	2025-10-06T13:46:57.538544Z	2025-10-06T13:47:10.157108Z
87	3	2025-10-06T13:59:16.080516Z	2025-10-06T13:59:16.080516Z
88	2	2025-10-06T20:28:23.064370Z	2025-10-06T20:28:44.222856Z
89	1	2025-10-06T20:33:37.845660Z	2025-10-06T20:33:37.845660Z
90	1	2025-10-06T20:59:38.170196Z	2025-10-06T20:59:38.170196Z
91	1	2025-10-10T03:55:47.993396Z	2025-10-10T03:55:47.993396Z

Session ID	Event Count	First Time	Last Time
92	1	2025-10-12T22:32:50.651618Z	2025-10-12T22:32:50.651618Z
93	1	2025-10-13T20:51:43.563734Z	2025-10-13T20:51:43.563734Z
94	1	2025-10-13T21:00:48.012926Z	2025-10-13T21:00:48.012926Z
95	1	2025-10-15T17:28:52.179316Z	2025-10-15T17:28:52.179316Z
96	2	2025-10-15T19:22:47.689678Z	2025-10-15T19:22:47.689678Z
97	1	2025-10-16T17:22:20.799852Z	2025-10-16T17:22:20.799852Z
98	1	2025-10-18T19:19:24.139156Z	2025-10-18T19:19:24.139156Z
99	5	2025-10-21T01:00:35.389485Z	2025-10-21T01:00:43.557250Z
100	1	2025-10-30T16:59:53.986162Z	2025-10-30T16:59:53.986162Z
101	6	2025-10-30T17:02:44.191176Z	2025-10-30T17:05:38.842196Z
102	1	2025-10-30T17:12:43.251456Z	2025-10-30T17:12:43.251456Z
103	2	2025-10-30T17:15:02.641636Z	2025-10-30T17:15:08.057736Z
104	2	2025-10-30T17:22:02.433046Z	2025-10-30T17:22:02.434054Z
105	3	2025-10-30T17:29:26.074946Z	2025-10-30T17:30:04.295754Z
106	1	2025-10-30T17:37:48.814388Z	2025-10-30T17:37:48.814388Z
107	4	2025-10-30T17:41:31.673464Z	2025-10-30T17:41:57.481320Z
108	3	2025-10-30T17:47:12.560040Z	2025-10-30T17:48:28.511676Z
109	1	2025-10-30T17:53:59.471024Z	2025-10-30T17:53:59.471024Z
110	4	2025-10-30T18:05:01.492812Z	2025-10-30T18:06:34.021386Z
111	10	2025-10-30T18:19:54.197000Z	2025-10-30T18:24:00.768690Z
112	4	2025-10-30T18:33:52.523340Z	2025-10-30T18:36:26.333752Z
113	1	2025-10-30T18:43:54.045796Z	2025-10-30T18:43:54.045796Z
114	14	2025-10-30T18:49:55.242320Z	2025-10-30T18:54:37.851092Z
115	1	2025-10-30T18:59:29.224234Z	2025-10-30T18:59:29.224234Z
116	1	2025-10-30T19:04:11.734794Z	2025-10-30T19:04:11.734794Z
117	3	2025-10-30T19:12:50.391126Z	2025-10-30T19:14:37.507456Z
118	2	2025-10-30T19:18:29.635106Z	2025-10-30T19:18:29.635106Z
119	8	2025-10-30T19:26:28.704408Z	2025-10-30T19:29:15.825000Z
120	1	2025-10-30T19:32:48.462974Z	2025-10-30T19:32:48.462974Z
121	2	2025-10-30T19:42:12.816538Z	2025-10-30T19:42:12.817572Z
122	8	2025-10-30T19:51:52.626652Z	2025-10-30T19:53:25.062140Z
123	7	2025-10-30T20:02:49.043720Z	2025-10-30T20:03:34.928596Z
124	3	2025-10-30T20:05:41.855632Z	2025-10-30T20:06:25.676634Z
125	4	2025-10-30T20:11:40.893622Z	2025-10-30T20:11:47.218724Z
126	1	2025-10-30T20:19:02.531220Z	2025-10-30T20:19:02.531220Z
127	5	2025-10-30T20:32:33.529998Z	2025-10-30T20:36:16.854100Z
128	5	2025-10-30T20:39:24.241810Z	2025-10-30T20:40:26.800488Z
129	5	2025-10-30T20:48:57.251014Z	2025-10-30T20:49:34.974976Z
130	7	2025-10-30T20:53:33.725170Z	2025-10-30T20:54:44.737912Z

Session ID	Event Count	First Time	Last Time
131	4	2025-10-30T20:57:36.044514Z	2025-10-30T20:59:26.755540Z
132	5	2025-10-30T21:24:33.519926Z	2025-10-30T21:25:30.254004Z
133	2	2025-10-30T21:28:31.525634Z	2025-10-30T21:28:31.525634Z
134	7	2025-10-31T16:05:19.313236Z	2025-10-31T16:08:44.345288Z
135	2	2025-10-31T16:11:13.786612Z	2025-10-31T16:11:13.786612Z
136	4	2025-10-31T16:13:32.784008Z	2025-10-31T16:13:58.141378Z
137	2	2025-10-31T16:25:44.742898Z	2025-10-31T16:25:44.742898Z
138	9	2025-10-31T16:51:59.038590Z	2025-10-31T16:54:57.571618Z
139	3	2025-10-31T16:57:38.728052Z	2025-10-31T16:57:46.910506Z
140	1	2025-10-31T17:14:49.171548Z	2025-10-31T17:14:49.171548Z
141	11	2025-10-31T17:17:14.285378Z	2025-10-31T17:19:11.421654Z
142	14	2025-10-31T18:09:37.288820Z	2025-10-31T18:12:35.257534Z
143	1	2025-10-31T18:15:20.444332Z	2025-10-31T18:15:20.444332Z
144	15	2025-11-03T10:03:01.065398Z	2025-11-03T10:04:29.416540Z
145	2	2025-11-03T10:11:05.114692Z	2025-11-03T10:11:11.163172Z
146	1	2025-11-05T04:59:59.719526Z	2025-11-05T04:59:59.719526Z
147	3	2025-11-06T07:02:53.801418Z	2025-11-06T07:02:58.263346Z
148	1	2025-11-06T07:08:34.169740Z	2025-11-06T07:08:34.169740Z
149	2	2025-11-07T09:14:58.373532Z	2025-11-07T09:15:05.461324Z
150	3	2025-11-07T09:26:15.873020Z	2025-11-07T09:26:15.873020Z
151	5	2025-11-08T16:37:07.513206Z	2025-11-08T16:39:08.489714Z
152	2	2025-11-08T16:51:27.640928Z	2025-11-08T16:51:27.640928Z
153	1	2025-11-08T16:53:55.501734Z	2025-11-08T16:53:55.501734Z
154	1	2025-11-08T17:50:58.569520Z	2025-11-08T17:50:58.569520Z
155	15	2025-11-08T18:36:41.806620Z	2025-11-08T18:39:47.714840Z
156	18	2025-11-08T18:43:31.880818Z	2025-11-08T18:49:21.311226Z
157	1	2025-11-10T05:54:04.401262Z	2025-11-10T05:54:04.401262Z
158	1	2025-11-10T06:41:52.635626Z	2025-11-10T06:41:52.635626Z
159	4	2025-11-10T13:10:17.374870Z	2025-11-10T13:10:59.307098Z
160	3	2025-11-10T18:46:23.738558Z	2025-11-10T18:46:39.680066Z
161	3	2025-11-11T12:47:07.492312Z	2025-11-11T12:49:12.532374Z
162	3	2025-11-13T08:19:03.669359Z	2025-11-13T08:19:03.669359Z
163	2	2025-11-14T06:32:54.510524Z	2025-11-14T06:34:15.906326Z
164	1	2025-11-14T06:52:35.402552Z	2025-11-14T06:52:35.402552Z
165	1	2025-11-14T07:20:31.343298Z	2025-11-14T07:20:31.343298Z
166	1	2025-11-14T08:00:55.262038Z	2025-11-14T08:00:55.262038Z
167	5	2025-11-14T08:11:30.858354Z	2025-11-14T08:11:39.821632Z
168	1	2025-11-14T08:33:07.063266Z	2025-11-14T08:33:07.063266Z
169	3	2025-11-14T09:51:47.350239Z	2025-11-14T09:51:47.350239Z

Session ID	Event Count	First Time	Last Time
170	1	2025-11-14T10:36:39.301934Z	2025-11-14T10:36:39.301934Z
171	3	2025-11-17T05:41:28.732138Z	2025-11-17T05:42:07.569668Z
172	1	2025-11-17T05:46:26.431738Z	2025-11-17T05:46:26.431738Z
173	1	2025-11-17T07:12:03.190438Z	2025-11-17T07:12:03.190438Z
174	2	2025-11-19T11:35:24.993288Z	2025-11-19T11:35:24.993288Z
175	1	2025-11-20T18:11:11.253434Z	2025-11-20T18:11:11.253434Z
176	3	2025-11-20T21:02:00.266789Z	2025-11-20T21:02:00.266789Z
177	1	2025-11-20T21:39:22.646124Z	2025-11-20T21:39:22.646124Z
178	2	2025-11-21T07:13:10.423844Z	2025-11-21T07:13:10.423844Z
179	2	2025-11-21T08:37:12.182326Z	2025-11-21T08:37:12.182326Z
180	1	2025-11-23T12:02:51.319150Z	2025-11-23T12:02:51.319150Z
181	1	2025-11-23T16:06:42.405632Z	2025-11-23T16:06:42.405632Z
182	1	2025-11-25T22:27:51.314470Z	2025-11-25T22:27:51.314470Z
183	1	2025-11-25T22:43:06.927280Z	2025-11-25T22:43:06.927280Z
184	1	2025-11-25T23:00:34.751816Z	2025-11-25T23:00:34.751816Z
185	1	2025-11-26T08:23:58.465632Z	2025-11-26T08:23:58.465632Z
186	3	2025-11-26T16:41:53.243976Z	2025-11-26T16:42:00.968982Z
187	2	2025-11-26T18:33:12.855784Z	2025-11-26T18:33:12.855784Z
188	1	2025-11-27T12:17:32.952032Z	2025-11-27T12:17:32.952032Z
189	2	2025-11-29T17:30:37.136894Z	2025-11-29T17:30:49.285212Z
190	3	2025-11-29T17:32:51.384456Z	2025-11-29T17:34:36.544640Z
191	1	2025-12-01T20:32:47.002380Z	2025-12-01T20:32:47.002380Z
192	1	2025-12-03T08:20:13.556672Z	2025-12-03T08:20:13.556672Z
193	1	2025-12-03T08:30:33.231010Z	2025-12-03T08:30:33.231010Z
194	1	2025-12-03T08:44:35.861976Z	2025-12-03T08:44:35.861976Z
195	1	2025-12-06T11:11:44.445714Z	2025-12-06T11:11:44.445714Z
196	1	2025-12-06T11:16:32.259188Z	2025-12-06T11:16:32.259188Z
197	4	2025-12-06T17:48:04.907976Z	2025-12-06T17:50:05.667884Z
198	1	2025-12-06T18:13:08.029340Z	2025-12-06T18:13:08.029340Z
199	1	2025-12-06T18:55:26.689016Z	2025-12-06T18:55:26.689016Z
200	1	2025-12-06T19:06:03.171898Z	2025-12-06T19:06:03.171898Z
201	4	2025-12-06T21:20:51.741796Z	2025-12-06T21:21:42.649580Z
202	1	2025-12-06T21:26:30.071836Z	2025-12-06T21:26:30.071836Z
203	4	2025-12-06T21:28:50.680166Z	2025-12-06T21:28:59.701004Z
204	1	2025-12-06T21:53:15.373612Z	2025-12-06T21:53:15.373612Z
205	1	2025-12-06T21:56:42.245108Z	2025-12-06T21:56:42.245108Z
206	1	2025-12-06T22:58:12.645536Z	2025-12-06T22:58:12.645536Z
207	1	2025-12-07T21:09:56.284408Z	2025-12-07T21:09:56.284408Z
208	2	2025-12-07T21:14:27.790326Z	2025-12-07T21:14:27.791322Z

Session ID	Event Count	First Time	Last Time
209	2	2025-12-07T21:19:33.288552Z	2025-12-07T21:19:33.288552Z
210	3	2025-12-07T21:44:15.191589Z	2025-12-07T21:44:15.191589Z
211	6	2025-12-07T21:50:55.243917Z	2025-12-07T21:50:55.318489Z
212	1	2025-12-07T22:32:31.379252Z	2025-12-07T22:32:31.379252Z
213	1	2025-12-07T22:37:14.527568Z	2025-12-07T22:37:14.527568Z
214	2	2025-12-08T05:16:11.461426Z	2025-12-08T05:16:11.461426Z
215	6	2025-12-08T05:25:40.652279Z	2025-12-08T05:26:07.401592Z
216	2	2025-12-08T05:41:30.743056Z	2025-12-08T05:41:30.743056Z
217	1	2025-12-08T07:06:33.167148Z	2025-12-08T07:06:33.167148Z
218	1	2025-12-08T07:21:41.649832Z	2025-12-08T07:21:41.649832Z
219	3	2025-12-08T07:28:38.279487Z	2025-12-08T07:28:38.279487Z
220	3	2025-12-08T20:57:27.444067Z	2025-12-08T20:57:27.444067Z
221	3	2025-12-08T21:56:30.279589Z	2025-12-08T21:56:30.279589Z
222	4	2025-12-08T22:18:08.454062Z	2025-12-08T22:18:27.075612Z
223	1	2025-12-08T22:46:01.053728Z	2025-12-08T22:46:01.053728Z
224	1	2025-12-08T22:59:03.524192Z	2025-12-08T22:59:03.524192Z
225	3	2025-12-08T23:07:36.678636Z	2025-12-08T23:07:36.678636Z
226	2	2025-12-08T23:23:21.307004Z	2025-12-08T23:23:22.987682Z
227	6	2025-12-08T23:41:28.339852Z	2025-12-08T23:42:05.877504Z
228	1	2025-12-08T23:44:07.328122Z	2025-12-08T23:44:07.328122Z
229	1	2025-12-09T00:02:08.003182Z	2025-12-09T00:02:08.003182Z
230	1	2025-12-09T00:16:50.417496Z	2025-12-09T00:16:50.417496Z
231	1	2025-12-09T00:20:14.985478Z	2025-12-09T00:20:14.985478Z
232	2	2025-12-09T00:22:28.877902Z	2025-12-09T00:22:28.878830Z
233	1	2025-12-09T00:27:25.063418Z	2025-12-09T00:27:25.063418Z
234	3	2025-12-09T00:56:54.947511Z	2025-12-09T00:56:54.947511Z
235	3	2025-12-09T01:01:56.330979Z	2025-12-09T01:01:56.330979Z
236	5	2025-12-09T01:23:59.075586Z	2025-12-09T01:25:06.929000Z
237	1	2025-12-09T01:37:29.105494Z	2025-12-09T01:37:29.105494Z
238	2	2025-12-09T01:58:03.171970Z	2025-12-09T01:58:04.403418Z
239	5	2025-12-09T10:43:05.390878Z	2025-12-09T10:45:10.460784Z
240	2	2025-12-09T11:53:08.085106Z	2025-12-09T11:53:08.085106Z
241	3	2025-12-09T12:01:28.545842Z	2025-12-09T12:01:28.545842Z
242	6	2025-12-09T13:05:19.467613Z	2025-12-09T13:05:19.590136Z
243	15	2025-12-09T14:19:31.734142Z	2025-12-09T14:20:51.249051Z
244	3	2025-12-09T14:30:03.568249Z	2025-12-09T14:30:03.568249Z
245	3	2025-12-09T14:35:36.288606Z	2025-12-09T14:35:36.288606Z
246	3	2025-12-09T14:43:48.893241Z	2025-12-09T14:43:48.893241Z
247	35	2025-12-09T15:26:58.331120Z	2025-12-09T15:29:57.122187Z

Session ID	Event Count	First Time	Last Time
248	3	2025-12-09T15:32:09.258592Z	2025-12-09T15:32:54.034306Z
249	1	2025-12-09T15:43:10.267416Z	2025-12-09T15:43:10.267416Z
250	2	2025-12-09T15:47:54.141574Z	2025-12-09T15:47:55.501616Z
251	17	2025-12-09T15:55:55.866000Z	2025-12-09T15:57:18.504000Z
252	3	2025-12-09T16:03:20.919135Z	2025-12-09T16:03:20.919135Z
253	3	2025-12-09T16:22:31.954624Z	2025-12-09T16:22:31.954624Z
254	1	2025-12-09T18:21:24.238498Z	2025-12-09T18:21:24.238498Z
255	1	2025-12-09T18:23:28.393594Z	2025-12-09T18:23:28.393594Z
256	3	2025-12-09T18:33:17.428551Z	2025-12-09T18:33:17.428551Z
257	3	2025-12-09T18:41:13.390971Z	2025-12-09T18:41:13.390971Z
258	3	2025-12-09T19:20:29.765537Z	2025-12-09T19:20:29.765537Z
259	16	2025-12-09T19:24:21.852364Z	2025-12-09T19:26:28.248000Z
260	3	2025-12-09T19:31:49.239466Z	2025-12-09T19:31:49.239466Z
261	37	2025-12-09T19:46:51.708164Z	2025-12-09T19:52:48.710203Z
262	5	2025-12-09T19:57:21.820400Z	2025-12-09T19:58:32.838806Z

Session Details (chronological)

Session 1 — 12 event(s)

Time	Type	Detail	Anomaly
2022-11-04T17:31:18.544000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $I0YNH6Q.win \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I0YNH6Q.win	
2022-11-04T17:31:18.544000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $I0YNH6Q.win \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I0YNH6Q.win	
2022-11-04T17:32:14.601000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $I88HIE0.c \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I88HIE0.c	
2022-11-04T17:32:14.601000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $ICDRVFV.exe \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ICDRVFV.exe	
2022-11-04T17:32:14.601000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $I88HIE0.c \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I88HIE0.c	
2022-11-04T17:32:14.601000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $ICDRVFV.exe \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ICDRVFV.exe	
2022-11-04T17:32:14.616000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $ID1EKZL.o \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ID1EKZL.o	
2022-11-04T17:32:14.616000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $ID1EKZL.o \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ID1EKZL.o	

Time	Type	Detail	Anomaly
2022-11-04T17:32:14.621000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $IIEVGNR.win \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IIEVGNR.win	
2022-11-04T17:32:14.621000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $IIEVGNR.win \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IIEVGNR.win	
2022-11-04T17:32:17.355000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $IEP3YK1.layout \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IEP3YK1.layout	
2022-11-04T17:32:17.355000Z	recycle_i	[Session 1] ■ Recycle Bin (deleted file) $IEP3YK1.layout \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IEP3YK1.layout	

Session 2 — 1 event(s)

Time	Type	Detail	Anomaly
2022-12-06T07:56:39.753000Z	recycle_i	[Session 2] ■ Recycle Bin (deleted file) $INNBR7G.jpg \| C:/$Recycle.Bin\S-1-5-21-509071697-2027520391-1498176977-1001\$INNBR7G.jpg	

Session 3 — 4 event(s)

Time	Type	Detail	Anomaly
2022-12-13T18:28:54.904980Z	lnk	[Session 3] ■ Shortcut / LNK Console RAR manual.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\WinRAR\Console RAR manual.lnk | target=C:\Program Files\WinRAR\Rar.txt | source=pylnk3	
2022-12-13T18:28:54.904980Z	lnk	[Session 3] ■ Shortcut / LNK What is new in the latest version.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\WinRAR\What is new in the latest version.lnk | target=C:\Program Files\WinRAR\WhatsNew.txt | source=pylnk3	
2022-12-13T18:28:54.904980Z	lnk	[Session 3] ■ Shortcut / LNK WinRAR help.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\WinRAR\WinRAR help.lnk | target=C:\Program Files\WinRAR\WinRAR.chm | source=pylnk3	
2022-12-13T18:28:54.904980Z	lnk	[Session 3] ■ Shortcut / LNK WinRAR.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\WinRAR\WinRAR.lnk | target=C:\Program Files\WinRAR\WinRAR.exe | source=pylnk3	

Session 4 — 1 event(s)

Time	Type	Detail	Anomaly
2023-02-11T09:34:13.716330Z	lnk	[Session 4] ■ Shortcut / LNK BlueJeans.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\BlueJeans.lnk | target=C:\Users\mukul\AppData\Local\BlueJeans\BlueJeans.exe | source=pylnk3	

Session 5 — 1 event(s)

Time	Type	Detail	Anomaly
2023-08-26T10:28:55.246372Z	lnk	[Session 5] ■ Shortcut / LNK MinGW Installation Manager.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\MinGW Installation Manager.lnk | target=C:\MinGW\libexec\mingw-get\guimain.exe | source=pylnk3	

Session 6 — 1 event(s)

Time	Type	Detail	Anomaly
2024-02-12T10:33:17.423267Z	lnk	[Session 6] ■ Shortcut / LNK emu8086.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\SendTo\emu8086.lnk | target=C:\emu8086\emu8086.exe | source=pylnk3	

Session 7 — 1 event(s)

Time	Type	Detail	Anomaly
2024-03-15T11:12:41.800748Z	lnk	[Session 7] ■ Shortcut / LNK balenaEtcher.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\balenaEtcher.lnk | target=C:\Users\mukul\AppData\Local\Programs\balena-etcher\balenaEtcher.exe | source=pylnk3	

Session 8 — 12 event(s)

Time	Type	Detail	Anomaly
2024-04-01T07:22:07.044074Z	lnk	[Session 8] ■ Shortcut / LNK Administrative Tools.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Administrative Tools.lnk | target=%windir%\system32\control.exe | source=pylnk3	
2024-04-01T07:22:07.044074Z	lnk	[Session 8] ■ Shortcut / LNK File Explorer.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\File Explorer.lnk | target=%UNKNOWN {52205FD8-5DFB-447D-801A-D0B52F2E83E1}% | source=pylnk3	
2024-04-01T07:22:07.856598Z	lnk	[Session 8] ■ Shortcut / LNK Command Prompt.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\System Tools\Command Prompt.lnk | target=%windir%\system32\cmd.exe | source=pylnk3	
2024-04-01T07:22:32.731763Z	lnk	[Session 8] ■ Shortcut / LNK Run.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\System Tools\Run.lnk | target=%UNKNOWN {2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}% | source=pylnk3	
2024-04-01T07:22:33.278666Z	lnk	[Session 8] ■ Shortcut / LNK LiveCaptions.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Accessibility\LiveCaptions.lnk | target=%windir%\system32\LiveCaptions.exe | source=pylnk3	
2024-04-01T07:22:33.294273Z	lnk	[Session 8] ■ Shortcut / LNK On-Screen Keyboard.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Accessibility\On-Screen Keyboard.lnk | target=%windir%\system32\osk.exe | source=pylnk3	

Time	Type	Detail	Anomaly
2024-04-01T07:22:33.309898Z	lnk	[Session 8] ■ Shortcut / LNK VoiceAccess.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Accessibility\VoiceAccess.lnk | target=%windir%\system32\voiceaccess.exe | source=pylnk3	
2024-04-01T07:22:39.403675Z	lnk	[Session 8] ■ Shortcut / LNK Control Panel.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\System Tools\Control Panel.lnk | target=%UNKNOWN {5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}% | source=pylnk3	
2024-04-01T07:22:39.497435Z	lnk	[Session 8] ■ Shortcut / LNK Magnify.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Accessibility\Magnify.lnk | target=%windir%\system32\magnify.exe | source=pylnk3	
2024-04-01T07:22:39.497435Z	lnk	[Session 8] ■ Shortcut / LNK Narrator.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Accessibility\Narrator.lnk | target=%windir%\system32\narrator.exe | source=pylnk3	
2024-04-01T07:24:04.090008Z	lnk	[Session 8] ■ Shortcut / LNK Windows PowerShell (x86).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell (x86).lnk | target=C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | source=pylnk3	
2024-04-01T07:24:04.090008Z	lnk	[Session 8] ■ Shortcut / LNK Windows PowerShell.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell.lnk | target=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | source=pylnk3	

Session 9 — 2 event(s)

Time	Type	Detail	Anomaly
2024-06-17T04:29:36.473032Z	lnk	[Session 9] ■ Shortcut / LNK Zoom Workplace.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Zoom\Zoom Workplace.lnk | target=C:\Users\mukul\AppData\Roaming\Zoom\bin\Zoom.exe | source=pylnk3	
2024-06-17T04:29:49.214784Z	lnk	[Session 9] ■ Shortcut / LNK Uninstall Zoom Workplace.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Zoom\Uninstall Zoom Workplace.lnk | target=C:\Users\mukul\AppData\Roaming\Zoom\uninstall\Installer.exe | source=pylnk3	

Session 10 — 2 event(s)

Time	Type	Detail	Anomaly
2024-07-23T06:04:45.420000Z	recycle_i	[Session 10] ■ Recycle Bin (deleted file) $ITINZ4G.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ITINZ4G.pdf	
2024-07-23T06:04:45.420000Z	recycle_i	[Session 10] ■ Recycle Bin (deleted file) $ITINZ4G.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ITINZ4G.pdf	

Session 11 — 4 event(s)

Time	Type	Detail	Anomaly
2024-08-05T09:26:46.737000Z	recycle_i	[Session 11] ■ Recycle Bin (deleted file) $I7UD30Y.jpg \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I7UD30Y.jpg	
2024-08-05T09:26:46.737000Z	recycle_i	[Session 11] ■ Recycle Bin (deleted file) $I7UD30Y.jpg \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I7UD30Y.jpg	
2024-08-05T09:26:46.746000Z	recycle_i	[Session 11] ■ Recycle Bin (deleted file) $IZY3WP5 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IZY3WP5	
2024-08-05T09:26:46.746000Z	recycle_i	[Session 11] ■ Recycle Bin (deleted file) $IZY3WP5 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IZY3WP5	

Session 12 — 2 event(s)

Time	Type	Detail	Anomaly
2024-08-05T09:30:15.313000Z	recycle_i	[Session 12] ■ Recycle Bin (deleted file) $IH4UM5E.jpg \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IH4UM5E.jpg	
2024-08-05T09:30:15.313000Z	recycle_i	[Session 12] ■ Recycle Bin (deleted file) $IH4UM5E.jpg \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IH4UM5E.jpg	

Session 13 — 1 event(s)

Time	Type	Detail	Anomaly
2024-08-28T07:05:54.284000Z	recycle_i	[Session 13] ■ Recycle Bin (deleted file) $IP4IAP8.nbi \| C:/$Recycle.Bin\S-1-5-21-509071697-2027520391-1498176977-1001\$IP4IAP8.nbi	

Session 14 — 1 event(s)

Time	Type	Detail	Anomaly
2024-08-29T10:33:38.299592Z	lnk	[Session 14] ■ Shortcut / LNK Nmap - Zenmap GUI.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Nmap\Nmap - Zenmap GUI.lnk | target=C:\Program Files (x86)\Nmap\zenmap\bin\pythonw.exe | source=pylnk3	

Session 15 — 4 event(s)

Time	Type	Detail	Anomaly
2024-08-30T05:35:59.687410Z	lnk	[Session 15] ■ Shortcut / LNK Python 3.12 (64-bit).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Python 3.12\Python 3.12 (64-bit).lnk | target=C:\Users\mukul\AppData\Local\Programs\Python\Python312\python.exe | source=pylnk3	
2024-08-30T05:36:19.605009Z	lnk	[Session 15] ■ Shortcut / LNK Python 3.12 Manuals (64-bit).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Python 3.12\Python 3.12 Manuals (64-bit).lnk | target=C:\Users\mukul\AppData\Local\Programs\Python\Python312\Doc\html\index.html | source=pylnk3	
2024-08-30T05:36:27.930492Z	lnk	[Session 15] ■ Shortcut / LNK IDLE (Python 3.12 64-bit).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Python 3.12\IDLE (Python 3.12 64-bit).lnk | target=C:\Users\mukul\AppData\Local\Programs\Python\Python312\pythonw.exe | source=pylnk3	
2024-08-30T05:36:28.123795Z	lnk	[Session 15] ■ Shortcut / LNK Python 3.12 Module Docs (64-bit).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Python 3.12\Python 3.12 Module Docs (64-bit).lnk | target=C:\Users\mukul\AppData\Local\Programs\Python\Python312\python.exe | source=pylnk3	

Session 16 — 2 event(s)

Time	Type	Detail	Anomaly
2024-12-12T16:00:58.080000Z	recycle_i	[Session 16] ■ Recycle Bin (deleted file) $ICQT8OI.py \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ICQT8OI.py	
2024-12-12T16:00:58.080000Z	recycle_i	[Session 16] ■ Recycle Bin (deleted file) $ICQT8OI.py \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$ICQT8OI.py	

Session 17 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-09T07:47:51.608726Z	lnk	[Session 17] ■ Shortcut / LNK Eclipse IDE for Enterprise Java and Web Developers - 2024-09.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Eclipse\Eclipse IDE for Enterprise Java and Web Developers - 2024-09.lnk | target=C:\Users\mukul\eclipse\jee-2024-09\eclipse\eclipse.exe | source=pylnk3	

Session 18 — 546 event(s)

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.688004Z	shellbag	[Session 18] ■ Folder Viewed e and Thunder | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \e and Thunder | source=registry	
2025-01-14T16:02:27.688004Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.690008Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.690008Z	shellbag	[Session 18] ■ Folder Viewed E01-08 WebRip 720p Hindi AAC 5.1 x264 ESub - mkvCinemas [Telly] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ E01-08 WebRip 720p Hindi AAC 5.1 x264 ESub - mkvCinemas [Telly] | source=registry	
2025-01-14T16:02:27.690008Z	shellbag	[Session 18] ■ Folder Viewed ch SO1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ch SO1 | source=registry	
2025-01-14T16:02:27.690008Z	shellbag	[Session 18] ■ Folder Viewed ch | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ch | source=registry	
2025-01-14T16:02:27.690008Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.692012Z	shellbag	[Session 18] ■ Folder Viewed Andreas | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\Andreas | source=registry	
2025-01-14T16:02:27.692012Z	shellbag	[Session 18] ■ Folder Viewed s Cricket 2007 + Cricket 2015 Patch - pRo | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\s Cricket 2007 + Cricket 2015 Patch - pRo | source=registry	
2025-01-14T16:02:27.692012Z	shellbag	[Session 18] ■ Folder Viewed s Cricket 2007 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\s Cricket 2007 + Cricket 2015 Patch - pRo\s Cricket 2007 | source=registry	
2025-01-14T16:02:27.692012Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\s Cricket 2007 + Cricket 2015 Patch - pRo\s Cricket 2007\ | source=registry	
2025-01-14T16:02:27.692012Z	shellbag	[Session 18] ■ Folder Viewed os ICC CWC 2015 Patch | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\s Cricket 2007 + Cricket 2015 Patch - pRo\os ICC CWC 2015 Patch | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\s Cricket 2007 + Cricket 2015 Patch - pRo\os ICC CWC 2015 Patch\s | source=registry	
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ | source=registry	
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed s's Creed 4 - Black Flag [FitGirl pc game] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\s's Creed 4 - Black Flag [FitGirl pc game] | source=registry	
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed s's Creed 4 - Black Flag [FitGirl Repack] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\s's Creed 4 - Black Flag [FitGirl pc game]\s's Creed 4 - Black Flag [FitGirl Repack] | source=registry	
2025-01-14T16:02:27.694016Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\s's Creed 4 - Black Flag [FitGirl pc game]\s's Creed 4 - Black Flag [FitGirl Repack]\■ | source=registry	
2025-01-14T16:02:27.696020Z	shellbag	[Session 18] ■ Folder Viewed Andreas | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \Andreas | source=registry	
2025-01-14T16:02:27.696020Z	shellbag	[Session 18] ■ Folder Viewed s's Creed 4 - Black Flag [FitGirl pc game] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\s's Creed 4 - Black Flag [FitGirl pc game] | source=registry	
2025-01-14T16:02:27.696020Z	shellbag	[Session 18] ■ Folder Viewed s's Creed 4 - Black Flag [FitGirl Repack] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\s's Creed 4 - Black Flag [FitGirl pc game]\s's Creed 4 - Black Flag [FitGirl Repack] | source=registry	
2025-01-14T16:02:27.696020Z	shellbag	[Session 18] ■ Folder Viewed s's Creed 4 - Black Flag | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \s's Creed 4 - Black Flag | source=registry	
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed 2TheFallofMaxpayne | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\2TheFallofMaxpayne | source=registry	
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed e 2 The Fall of Max payne | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\2TheFallofMaxpayne\e 2 The Fall of Max payne | source=registry	
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed e 2 The Fall of Max Payne | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\2TheFallofMaxpayne\e 2 The Fall of Max payne\e 2 The Fall of Max Payne | source=registry	
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\2TheFallofMaxpayne\e 2 The Fall of Max payne\@ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.698024Z	shellbag	[Session 18] ■ Folder Viewed ies.2.World.in.Flames.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ies.2.World.in.Flames.zip | source=registry	
2025-01-14T16:02:27.700028Z	shellbag	[Session 18] ■ Folder Viewed al | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\al | source=registry	
2025-01-14T16:02:27.701774Z	shellbag	[Session 18] ■ Folder Viewed +V0+V. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V. | source=registry	
2025-01-14T16:02:27.701774Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ | source=registry	
2025-01-14T16:02:27.701774Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.701774Z	shellbag	[Session 18] ■ Folder Viewed +V0+V0. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \+V0+V0. | source=registry	
2025-01-14T16:02:27.703778Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ | source=registry	
2025-01-14T16:02:27.703778Z	shellbag	[Session 18] ■ Folder Viewed JECT | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ \JECT | source=registry	
2025-01-14T16:02:27.703778Z	shellbag	[Session 18] ■ Folder Viewed ject | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ \JECT\ject | source=registry	
2025-01-14T16:02:27.703778Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ \ | source=registry	
2025-01-14T16:02:27.703778Z	shellbag	[Session 18] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \+V0+V.\ \l | source=registry	
2025-01-14T16:02:27.705782Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.705782Z	shellbag	[Session 18] ■ Folder Viewed ation | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ation | source=registry	
2025-01-14T16:02:27.705782Z	shellbag	[Session 18] ■ Folder Viewed terial | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ation\terial | source=registry	
2025-01-14T16:02:27.705782Z	shellbag	[Session 18] ■ Folder Viewed al | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \al | source=registry	
2025-01-14T16:02:27.705782Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \@ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.707786Z	shellbag	[Session 18] ■ Folder Viewed gR1_database_111070.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \gR1_database_111070.zip | source=registry	
2025-01-14T16:02:27.709790Z	shellbag	[Session 18] ■ Folder Viewed -3.0.3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \-3.0.3 | source=registry	
2025-01-14T16:02:27.709790Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \-3.0.3\-3.0.3\@ | source=registry	
2025-01-14T16:02:27.711794Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \-3.0.3\-3.0.3\@\■ | source=registry	
2025-01-14T16:02:27.713798Z	shellbag	[Session 18] ■ Folder Viewed -3.0.3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \-3.0.3\-3.0.3 | source=registry	
2025-01-14T16:02:27.713798Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \-3.0.3\-3.0.3\ | source=registry	
2025-01-14T16:02:27.713798Z	shellbag	[Session 18] ■ Folder Viewed staller_Portable.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \staller_Portable.zip | source=registry	
2025-01-14T16:02:27.715802Z	shellbag	[Session 18] ■ Folder Viewed staller_Portable | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \staller_Portable | source=registry	
2025-01-14T16:02:27.715802Z	shellbag	[Session 18] ■ Folder Viewed staller_Portable | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \staller_Portable\staller_Portable | source=registry	
2025-01-14T16:02:27.715802Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \staller_Portable\staller_Portable\■ | source=registry	
2025-01-14T16:02:27.717546Z	shellbag	[Session 18] ■ Folder Viewed 10 Pro 19H2 1909.18363.752 Preactivated March 2020 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \10 Pro 19H2 1909.18363.752 Preactivated March 2020 | source=registry	
2025-01-14T16:02:27.717546Z	shellbag	[Session 18] ■ Folder Viewed 10 Pro 19H2 1909.18363.752 Preactivated March 2020 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \10 Pro 19H2 1909.18363.752 Preactivated March 2020\10 Pro 19H2 1909.18363.752 Preactivated March 2020 | source=registry	
2025-01-14T16:02:27.717546Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \10 Pro 19H2 1909.18363.752 Preactivated March 2020\10 Pro 19H2 1909.18363.752 Preactivated March 2020\■ | source=registry	
2025-01-14T16:02:27.717546Z	shellbag	[Session 18] ■ Folder Viewed ux-2024.2-virtualbox-amd64 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ux-2024.2-virtualbox-amd64 | source=registry	
2025-01-14T16:02:27.717546Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.719550Z	shellbag	[Session 18] ■ Folder Viewed ux-2024.2-virtualbox-amd64 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ux-2024.2-virtualbox-amd64\ux-2024.2-virtualbox-amd64 | source=registry	
2025-01-14T16:02:27.719550Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \@ | source=registry	
2025-01-14T16:02:27.719550Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \@\ | source=registry	
2025-01-14T16:02:27.719550Z	shellbag	[Session 18] ■ Folder Viewed etup | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \etup | source=registry	
2025-01-14T16:02:27.719550Z	shellbag	[Session 18] ■ Folder Viewed 408.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \408.zip | source=registry	
2025-01-14T16:02:27.721554Z	shellbag	[Session 18] ■ Folder Viewed h | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \h | source=registry	
2025-01-14T16:02:27.721554Z	shellbag	[Session 18] ■ Folder Viewed h.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \h.zip | source=registry	
2025-01-14T16:02:27.725564Z	shellbag	[Session 18] ■ Folder Viewed eft Auto Vice City (Repack) - PC | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft Auto Vice City (Repack) - PC | source=registry	
2025-01-14T16:02:27.725564Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft Auto Vice City (Repack) - PC\@ | source=registry	
2025-01-14T16:02:27.725564Z	shellbag	[Session 18] ■ Folder Viewed City - Ultimate Pack Blood Patch | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft Auto Vice City (Repack) - PC\@\ City - Ultimate Pack Blood Patch | source=registry	
2025-01-14T16:02:27.727568Z	shellbag	[Session 18] ■ Folder Viewed indows-x64_bin | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \indows-x64_bin | source=registry	
2025-01-14T16:02:27.727568Z	shellbag	[Session 18] ■ Folder Viewed .2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \indows-x64_bin\.2 | source=registry	
2025-01-14T16:02:27.727568Z	shellbag	[Session 18] ■ Folder Viewed indows-x64_bin.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \indows-x64_bin.zip | source=registry	
2025-01-14T16:02:27.727568Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.729570Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.729570Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.729570Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\ | source=registry	
2025-01-14T16:02:27.729570Z	shellbag	[Session 18] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\ \er | source=registry	
2025-01-14T16:02:27.729570Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\ | source=registry	
2025-01-14T16:02:27.731574Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-14T16:02:27.731574Z	shellbag	[Session 18] ■ Folder Viewed Set-NFSU-SEM-II | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\ Set-NFSU-SEM-II | source=registry	
2025-01-14T16:02:27.731574Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.731574Z	shellbag	[Session 18] ■ Folder Viewed Duty Modern Warfare 3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Duty Modern Warfare 3 | source=registry	
2025-01-14T16:02:27.733320Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.733320Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.735322Z	shellbag	[Session 18] ■ Folder Viewed JECT | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \JECT | source=registry	
2025-01-14T16:02:27.735322Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.735322Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.735322Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.735322Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed eft Auto Vice City (Repack) - PC | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\eft Auto Vice City (Repack) - PC | source=registry	
2025-01-14T16:02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16: 02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16: 02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed ject | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \JECT\ject | source=registry	
2025-01-14T16: 02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16: 02:27.737326Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed Set-NFSU-SEM-II | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ Set-NFSU-SEM-II | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\eft Auto Vice City (Repack) - PC\@ | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed City - Ultimate Pack Blood Patch | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\eft Auto Vice City (Repack) - PC\@\ City - Ultimate Pack Blood Patch | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\eft Auto Vice City (Repack) - PC\@\> | source=registry	
2025-01-14T16: 02:27.739330Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\eft Auto Vice City (Repack) - PC\@\>\@ | source=registry	
2025-01-14T16: 02:27.741334Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\> | source=registry	
2025-01-14T16: 02:27.743338Z	shellbag	[Session 18] ■ Folder Viewed 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ 1 | source=registry	
2025-01-14T16: 02:27.743338Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16: 02:27.745340Z	shellbag	[Session 18] ■ Folder Viewed -5 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-5 | source=registry	
2025-01-14T16: 02:27.745340Z	shellbag	[Session 18] ■ Folder Viewed -3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-3 | source=registry	
2025-01-14T16: 02:27.745340Z	shellbag	[Session 18] ■ Folder Viewed -2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-2 | source=registry	

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-01-14T16:02:27.745340Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.745340Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\> | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed -8 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-8 | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.747344Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \er | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.749088Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.749088Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ \ \> | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
<tr><td>2025-01-14T16:02:27.751092Z</td><td>shellbag</td><td>[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry</td><td></td></tr>
</table>

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed notes 7 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \notes 7 | source=registry	
2025-01-14T16:02:27.753096Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.755100Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.755100Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\> | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed notes 7 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \notes 7 | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed -3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-3 | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed -2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-2 | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ 1 | source=registry	
2025-01-14T16:02:27.757104Z	shellbag	[Session 18] ■ Folder Viewed -5 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \-5 | source=registry	
2025-01-14T16:02:27.759108Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.759108Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.759108Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ | source=registry	
2025-01-14T16:02:27.759108Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \> | source=registry	
2025-01-14T16:02:27.759108Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ \ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \ \ \> | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.761112Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.764862Z	shellbag	[Session 18] ■ Folder Viewed pp1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \pp1 | source=registry	
2025-01-14T16:02:27.764862Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.764862Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■\■ | source=registry	
2025-01-14T16:02:27.764862Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.766864Z	shellbag	[Session 18] ■ Folder Viewed ctical List Solutions.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ctical List Solutions.zip | source=registry	
2025-01-14T16:02:27.766864Z	shellbag	[Session 18] ■ Folder Viewed pp2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \pp2 | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.766864Z	shellbag	[Session 18] ■ Folder Viewed pp2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \pp2\pp2 | source=registry	
2025-01-14T16:02:27.772876Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.772876Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■\■ | source=registry	
2025-01-14T16:02:27.774880Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.774880Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■\■ | source=registry	
2025-01-14T16:02:27.774880Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.774880Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.774880Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.776882Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.778886Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.778886Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.778886Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.778886Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.778886Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed l List Solutions | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \l List Solutions\■ | source=registry	
2025-01-14T16:02:27.780630Z	shellbag	[Session 18] ■ Folder Viewed ormsApp1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ormsApp1 | source=registry	
2025-01-14T16:02:27.782636Z	shellbag	[Session 18] ■ Folder Viewed nt-2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\nt-2 | source=registry	
2025-01-14T16:02:27.782636Z	shellbag	[Session 18] ■ Folder Viewed nt-1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\nt-1 | source=registry	
2025-01-14T16:02:27.784640Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■ | source=registry	
2025-01-14T16:02:27.784640Z	shellbag	[Session 18] ■ Folder Viewed l.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\l.zip | source=registry	
2025-01-14T16:02:27.784640Z	shellbag	[Session 18] ■ Folder Viewed ate | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ate | source=registry	
2025-01-14T16:02:27.784640Z	shellbag	[Session 18] ■ Folder Viewed redential_mukulsain.genai@gmail.com | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ate\redential_mukulsain.genai@gmail.com | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.784640Z	shellbag	[Session 18] ■ Folder Viewed redential_mukulsain.genai@gmail.com.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ate\redential_mukulsain.genai@gmail.com.zip | source=registry	
2025-01-14T16:02:27.786644Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.786644Z	shellbag	[Session 18] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\l | source=registry	
2025-01-14T16:02:27.786644Z	shellbag	[Session 18] ■ Folder Viewed ementation | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\l\ementation | source=registry	
2025-01-14T16:02:27.788648Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.788648Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.788648Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.788648Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.788648Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.790652Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■ | source=registry	
2025-01-14T16:02:27.790652Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.790652Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.790652Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.790652Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■ | source=registry	
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l | source=registry	
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed Pad | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\Pad | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed lysis | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\lysis | source=registry	
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed ipher | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\ipher | source=registry	
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed ellman Key Exchange | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\ellman Key Exchange | source=registry	
2025-01-14T16:02:27.792656Z	shellbag	[Session 18] ■ Folder Viewed onary Access Control | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\onary Access Control | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \> | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed ementation | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■\■\l\ementation | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\■ | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.794660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\ | source=registry	
2025-01-14T16:02:27.798408Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.798408Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.798408Z	shellbag	[Session 18] ■ Folder Viewed -20240719T004506Z-001.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\-20240719T004506Z-001.zip | source=registry	
2025-01-14T16:02:27.798408Z	shellbag	[Session 18] ■ Folder Viewed material.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\ material.zip | source=registry	
2025-01-14T16:02:27.800412Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.800412Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \@ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.800412Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.802416Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.802416Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.802416Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ | source=registry	
2025-01-14T16:02:27.804420Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ | source=registry	
2025-01-14T16:02:27.806424Z	shellbag	[Session 18] ■ Folder Viewed orts-master | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master | source=registry	
2025-01-14T16:02:27.806424Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \> | source=registry	
2025-01-14T16:02:27.806424Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \>\ | source=registry	
2025-01-14T16:02:27.808428Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■ | source=registry	
2025-01-14T16:02:27.808428Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■ | source=registry	
2025-01-14T16:02:27.808428Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.808428Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \■ | source=registry	
2025-01-14T16:02:27.810432Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ | source=registry	
2025-01-14T16:02:27.810432Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \ | source=registry	
2025-01-14T16:02:27.810432Z	shellbag	[Session 18] ■ Folder Viewed orts | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \ \orts | source=registry	
2025-01-14T16:02:27.810432Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \ \orts\■ | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed orts-master | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \s | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed orts | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \s\orts | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \s\orts\■ | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \s\orts\■\@ | source=registry	
2025-01-14T16:02:27.812176Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\■\ \s\orts\■\@\s | source=registry	
2025-01-14T16:02:27.814180Z	shellbag	[Session 18] ■ Folder Viewed po | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\po | source=registry	
2025-01-14T16:02:27.814180Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master\orts-master\po\■ | source=registry	
2025-01-14T16:02:27.816184Z	shellbag	[Session 18] ■ Folder Viewed orts-master.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \orts-master.zip | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed ication1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1 | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1\■ | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed ication1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1\■\ication1 | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1\■\■ | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1\ | source=registry	
2025-01-14T16:02:27.820192Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication1\ \@ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ication4 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4 | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4\■ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4\■\ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed orts | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4\■\ \orts | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ication4 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4\■\ication4 | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed t | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ication4\t | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\@ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed CN | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\@\CN | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed CN | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\CN | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed CN | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■\CN\CN | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ignment | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ignment | source=registry	
2025-01-14T16:02:27.822198Z	shellbag	[Session 18] ■ Folder Viewed ■W■W. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■W■W. | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed aan | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \aan | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\> | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■YTK%Y+. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■YTK%Y+. | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\d | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\d\■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\d\> | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\d | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\d\ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\ \@ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\■ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ch SO1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\■\ch SO1 | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\> | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\■ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d\■\l | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \@ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \d | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \d | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \d\> | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \l | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed er (2) | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\er (2) | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.827998Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed Files | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Files | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed leWindowsApps | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Files\leWindowsApps | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \.pdf\@ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ay | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \.pdf\ay | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed eft_Auto_V_GTA_5_RELOADED | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft_Auto_V_GTA_5_RELOADED | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed eft_Auto_V_GTA_5_RELOADED | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft_Auto_V_GTA_5_RELOADED\eft_Auto_V_GTA_5_RELOADED | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed eft_Auto_V_GTA_5_RELOADED.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eft_Auto_V_GTA_5_RELOADED.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ay | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ay | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ettter-2-1645608985174 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\ettter-2-1645608985174 | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed 718343744023 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\718343744023 | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \er | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed 718343744023 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\718343744023 | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed 08762233636 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\08762233636 | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed e_1718345109322.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\e_1718345109322.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed 718343744023.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\718343744023.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed 08762233636.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\08762233636.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed .zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed Studio | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Studio | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ettter-2-1645608985174 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ettter-2-1645608985174 | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ettter-2-1645608985174.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ettter-2-1645608985174.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed -20240719T004506Z-001.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\-20240719T004506Z-001.zip | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.843544Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed pps | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\pps | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\■ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\■\ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed n Teaser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \n Teaser | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed e 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \n Teaser\e 1 | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed allenge1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \allenge1 | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed allenge1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \allenge1\allenge1 | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed allenge2.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \allenge2.zip | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed d sbi malware.apk_Decompiler.com.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \d sbi malware.apk_Decompiler.com.zip | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed .zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \.zip | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed eFile | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eFile | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed eFile.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \eFile.zip | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ut | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ut | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed le Banner.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \le Banner.zip | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed {E04FD020000000000000000000000000} | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \le Banner.zip\CLSID\{E04FD020000000000000000000000000} | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ut.tar.gz | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ut.tar.gz | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed 1] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1] | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1]\1 | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1]\1\1 | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed database | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1]\database | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed tabase | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1]\tabase | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ■YTK■YTK. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■YTK■YTK. | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed] | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\] | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\]\@ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\]\■ | source=registry	
2025-01-14T16:02:27.859568Z	shellbag	[Session 18] ■ Folder Viewed 1].zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\1].zip | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ication1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ication1 | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed Python | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ \■ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ction | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ction | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ction\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ction\>\s | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ction\>\> | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\\ction\>\>\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed age | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\\ction\age | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\@ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed mages | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\@\mages | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed age | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\@\age | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \ \s | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\ \■ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\\■\er | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed mages | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\mages | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed age | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\Python\age | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\>\> | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\>\s | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\>\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\>\>\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \s | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ensorflow-example | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ensorflow-example | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ayer_tensorflow | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ayer_tensorflow | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed ayer | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ayer | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ayer\> | source=registry	
2025-01-14T16:02:27.875264Z	shellbag	[Session 18] ■ Folder Viewed e__ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \e__ | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed nnector-j-9.1.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nnector-j-9.1.0 | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed nnector-j-9.1.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nnector-j-9.1.0\nnector-j-9.1.0 | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed 23.0.1_windows-x64_bin.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\23.0.1_windows-x64_bin.zip | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ication1\■ | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed Examples | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ication1\■\Examples | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ux-2024.3-virtualbox-amd64 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ux-2024.3-virtualbox-amd64 | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ux-2024.3-virtualbox-amd64 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ux-2024.3-virtualbox-amd64\ux-2024.3-virtualbox-amd64 | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ismo-2023-film-691445.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ismo-2023-film-691445.zip | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed directory | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\directory | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed nt | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\directory\nt | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed unction | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\directory\unction | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed uY■uY■. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\directory\uY■uY■. | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed 2772_vpcflowlogs_eu-north-1_fl-0a2ec996a10cb4862_20241122T0040Z_21220ca3.log.gz | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\2772_vpcflowlogs_eu-north-1_fl-0a2ec996a10cb4862_20241122T0040Z_21220ca3.log.gz | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed 2772_vpcflowlogs_eu-north-1_fl-0a2ec996a10cb4862_20241121T2120Z_93255113.log | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\2772_vpcflowlogs_eu-north-1_fl-0a2ec996a10cb4862_20241121T2120Z_93255113.log | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed p | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\p | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed adCache | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\adCache | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed lUlU. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\lUlU. | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed ein- Enemy Territory | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\lUlU.\ein- Enemy Territory | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\lUlU.\ein- Enemy Territory\@ | source=registry	
2025-01-14T16:02:27.891212Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \> | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \>\@ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \>\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@\@ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■\ \@ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■\ \@\> | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■\ \@\>\ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@\■ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@\■\■ | source=registry	
2025-01-14T16:02:27.922660Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@\■ | source=registry	
2025-01-14T16:02:27.938360Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \ | source=registry	
2025-01-14T16:02:27.938360Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \ \■ | source=registry	
2025-01-14T16:02:27.943442Z	shellbag	[Session 18] ■ Folder Viewed f | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \f | source=registry	
2025-01-14T16:02:27.943442Z	shellbag	[Session 18] ■ Folder Viewed < | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \< | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed nu | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\@\t\@\nu | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\ \ | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed f | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \f | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@ | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@\ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@\ \ | source=registry	
2025-01-14T16:02:27.954480Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ata | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ata | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed t | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ata\t | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ata\t\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \■\■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \■\■\ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \■\■\ \■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \■\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\@ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\■\@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed .0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@\■\@\.0 | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \■ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \@ | source=registry	
2025-01-14T16:02:27.970382Z	shellbag	[Session 18] ■ Folder Viewed old | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\old | source=registry	
2025-01-14T16:02:27.986146Z	shellbag	[Session 18] ■ Folder Viewed nu | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ata\t\@\nu | source=registry	
2025-01-14T16:02:27.986146Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\P■■ 1■■■■■■■■■■■■■r■■■■■■■ ■■■R■■■■■R■e■d■m■i■ ■K■5■0■i■■■\■\■?■\■u■s■b■ #■v■i■d■_■2■7■1■7■&■p■i■d■_■f■f■4■0■#■s■s■h■e■d ■6■v■s■4■p■c■y■q■c■t■k■#■{■6■a■c■2■7■8■7■8■-■a ■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■ f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■R■e■d■m■i■ ■K■5■0■i■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:27.986146Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\X■■ 1■■■■■■■■■■■■■~■■■■■■■■■■■J■■■■■R■e■d■m■i ■ ■N■o■t■e■ ■9■ ■P■r■o■■■\■\■?■\■u■s■b■#■v■i■d■_ ■2■7■1■7■&■p■i■d■_■f■f■4■0■#■1■9■a■5■3■3■6■b■# ■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8 ■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■"■■■R■e■d■m■i■ ■N■o■t■e■ ■9■ ■P■r■o■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:27.986146Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\L■■ 1■■■■■■■■■■■■■p■■■■■■■ ■■■R■■■■■v■i■v■o■ ■1■8■2■0■■■\■\■?■\■u■s■b■#■v■i■d■_■2■d■9■5■&■p■i■d■_■6■0■0■2■#■a■a■n■7■7■t■t■g■w■4■e■a■t■w■g■q■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■v■i■v■o■ ■1■8■2■0■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed F:\ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\F:\ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\H■■ 1■■■■■■■■■■■■■n■■■■■■■ ■■■R■■■■■r■e■a■l■m■e■ ■7■■■\■\■?■\■u■s■b■#■v■i■d■_■0■e■8■d■&■p■i■d■_■2■0■0■8■#■h■e■k■b■l■j■g■u■x■4■a■m■y■9■f■e■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■r■e■a■l■m■e■ ■7■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\H■■ 1■■■■■■■■■■■■■n■■■■■■■ ■■■R■■■■■r■e■a■l■m■e■ ■7■■■\■\■?■\■u■s■b■#■v■i■d■_■0■e■8■d■&■p■i■d■_■2■0■0■b■#■h■e■k■b■l■j■g■u■x■4■a■m■y■9■f■e■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■r■e■a■l■m■e■ ■7■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\■■ 1■■■■■■■■■■■■■n■■■■■■■ ■■■o■■■■■C■h■i■n■m■a■y■i■■■\■\■?■\■u■s■b■#■v■i■d■_■0■4■e■8■&■p■i■d■_■6■8■6■0■&■m■s■_■c■o■m■p■_■m■t■p■&■s■a■m■s■u■n■g■_■a■n■d■r■o■i■d■#■6■&■3■0■9■1■3■c■a■4■&■2■&■0■0■0■0■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■C■h■i■n■m■a■y■i■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\N■■ 1■■■■■■■■■■■■■r■■■■■■■ ■■■Q■■■■■i■Q■O■O■■Z■6■ ■5■G■■■\■\■?■\■u■s■b■#■v■i■d■_■2■d■9■5■&■p■i■d■_■6■0■0■2■#■1■3■9■8■1■6■9■7■1■7■0■0■0■f■b■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■i■Q■O■O■ ■Z■6■■5■G■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\■■ 1■■■■■■■■■■■■■n■■■■■■■ ■■■o■■■■■C■h■i■n■m■a■y■i■■■\■\■?■\■u■s■b■#■v■i■d■_■0■4■e■8■&■p■i■d■_■6■8■6■0■&■m■s■_■c■o■m■p■_■m■t■p■&■s■a■m■s■u■n■g■_■a■n■d■r■o■i■d■#■6■&■3■0■9■1■3■c■a■4■&■1■&■0■0■0■0■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■C■h■i■n■m■a■y■i■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\d■■ 1■■■■■■■■■■■■■v■■■■■■■ ■■■X■■■■■A■p■p■l■e■ ■i■P■h■o■n■e■■■\■\■?■\■u■s■b■#■v■i■d■_■0■5■a■c■&■p■i■d■_■1■2■a■8■&■m■i■_■0■0■#■6■&■7■e■4■7■1■1■1■&■1■&■0■0■0■0■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■A■p■p■l■e■ ■i■P■h■o■n■e■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\d■■ 1■■■■■■■■■■■■■v■■■■■■■ ■■■X■■■■■A■p■p■l■e■ ■i■P■h■o■n■e■■■\■\■?■\■u■s■b■#■v■i■d■_■0■5■a■c■&■p■i■d■_■1■2■a■8■&■m■i■_■0■0■#■6■&■7■e■4■7■1■1■1■&■0■&■0■0■0■0■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■A■p■p■l■e■ ■i■P■h■o■n■e■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed +■ezFkp:■&■■■&■■■■■■■■■Tl8 ■■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\+■ezFkp:■&■■■&■■■■■■■■■Tl8 ■■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed h■■86■■W ■■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\:,LB)■A&■■■&■■■■■/h■■86■■W ■■ | source=registry	
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed :$i0E■Az&■■■&■■■■■■■■ "p■O■■ \| CLSID\{E04FD020EA3A6910A2D808002B30309D}\:$i0E■Az&■■■&■■■■■■■■ "p■O■■ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:28.001846Z	shellbag	[Session 18] ■ Folder Viewed ■9■#■■K&]B■_ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\■9■#■■K&]B■_ | source=registry	
2025-01-14T16:02:28.017664Z	shellbag	[Session 18] ■ Folder Viewed opO■F■:&■■■&■■■■■j■■?$p■}NQ■■ \| CLSID\{E04FD020EA3A6910A2D808002B30309D}\opO■F■:&■■■&■■■■■j■■?$p■}NQ■■ | source=registry	
2025-01-14T16:02:28.043714Z	shellbag	[Session 18] ■ Folder Viewed {CB859F6720028040B29B5540CC05AAB6} | CLSID\{CB859F6720028040B29B5540CC05AAB6} | source=registry	
2025-01-14T16:02:28.045718Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.047722Z	shellbag	[Session 18] ■ Folder Viewed .0-B | CLSID\{05398E082303024B98265D99428E115F}\.0-B | source=registry	
2025-01-14T16:02:28.047722Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{05398E082303024B98265D99428E115F}\> | source=registry	
2025-01-14T16:02:28.047722Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.047722Z	shellbag	[Session 18] ■ Folder Viewed .3(2 | CLSID\{05398E082303024B98265D99428E115F}\.3(2 | source=registry	
2025-01-14T16:02:28.049466Z	shellbag	[Session 18] ■ Folder Viewed .0-B | CLSID\{05398E082303024B98265D99428E115F}\.0-B\.0-B | source=registry	
2025-01-14T16:02:28.049466Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.049466Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.049466Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.051470Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.051470Z	shellbag	[Session 18] ■ Folder Viewed > | CLSID\{05398E082303024B98265D99428E115F}\> | source=registry	
2025-01-14T16:02:28.053474Z	shellbag	[Session 18] ■ Folder Viewed .ZIP | CLSID\{05398E082303024B98265D99428E115F}\.ZIP | source=registry	
2025-01-14T16:02:28.057482Z	shellbag	[Session 18] ■ Folder Viewed @ | CLSID\{2F0010B7A6F519002F453A5C00000000}\@ | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:28.059486Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{2F0010B7A6F519002F453A5C00000000}\■ | source=registry	
2025-01-14T16:02:28.059486Z	shellbag	[Session 18] ■ Folder Viewed ■ | CLSID\{2F0010B7A6F519002F453A5C00000000}\■\■ | source=registry	
2025-01-14T16:02:28.059486Z	shellbag	[Session 18] ■ Folder Viewed {2D02D5DFA3231F020400000000001B02} | CLSID\{2D02D5DFA3231F020400000000001B02} | source=registry	
2025-01-14T16:02:28.061490Z	shellbag	[Session 18] ■ Folder Viewed {2D02D5DFA3231F020400000000001B02} | CLSID\{2D02D5DFA3231F020400000000001B02} | source=registry	
2025-01-14T16:02:28.061490Z	shellbag	[Session 18] ■ Folder Viewed {5316DD3A32EBB04CBBD7DFA0ABB5ACCA} | CLSID\{5316DD3A32EBB04CBBD7DFA0ABB5ACCA} | source=registry	
2025-01-14T16:02:28.061490Z	shellbag	[Session 18] ■ Folder Viewed {1104D5DFA3230304000000000000FF03} | CLSID\{1104D5DFA3230304000000000000FF03} | source=registry	
2025-01-14T16:02:28.061490Z	shellbag	[Session 18] ■ Folder Viewed {1104D5DFA3230304000000000000FF03} | CLSID\{1104D5DFA3230304000000000000FF03} | source=registry	
2025-01-14T16:02:28.065238Z	shellbag	[Session 18] ■ Folder Viewed {6806EE260AA0D7449371BEB064C98683} | CLSID\{6806EE260AA0D7449371BEB064C98683} | source=registry	
2025-01-14T16:02:28.067242Z	shellbag	[Session 18] ■ Folder Viewed {8F00F01213212A4880B3FD5E91C12313} | CLSID\{8F00F01213212A4880B3FD5E91C12313} | source=registry	
2025-01-14T16:02:28.069254Z	shellbag	[Session 18] ■ Folder Viewed {E902D5DFA323DB02040000000000D702} | CLSID\{E902D5DFA323DB02040000000000D702} | source=registry	
2025-01-14T16:02:28.069254Z	shellbag	[Session 18] ■ Folder Viewed {E902D5DFA323DB02040000000000D702} | CLSID\{E902D5DFA323DB02040000000000D702} | source=registry	
2025-01-14T16:02:28.069254Z	shellbag	[Session 18] ■ Folder Viewed {8109D5DFA32373090400000000006F09} | CLSID\{8109D5DFA32373090400000000006F09} | source=registry	
2025-01-14T16:02:28.069254Z	shellbag	[Session 18] ■ Folder Viewed {8109D5DFA32373090400000000006F09} | CLSID\{8109D5DFA32373090400000000006F09} | source=registry	
2025-01-14T16:02:28.069254Z	shellbag	[Session 18] ■ Folder Viewed {96F2FD3DECDBB44F81D16A3438BCF4DE} | CLSID\{96F2FD3DECDBB44F81D16A3438BCF4DE} | source=registry	
2025-01-14T16:02:28.071258Z	shellbag	[Session 18] ■ Folder Viewed {0E3174F8B7B6DC47BC84B9E6B38F5903} | CLSID\{0E3174F8B7B6DC47BC84B9E6B38F5903} | source=registry	
2025-01-14T16:02:28.071258Z	shellbag	[Session 18] ■ Folder Viewed {3ACCBFB42CDB4C42B0297FE99A87C641} | CLSID\{3ACCBFB42CDB4C42B0297FE99A87C641} | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:28.071258Z	shellbag	[Session 18] ■ Folder Viewed {D1A4B4B254274041A2EB9A76D9D7CDC6} | CLSID\{D1A4B4B254274041A2EB9A76D9D7CDC6} | source=registry	
2025-01-14T16:02:28.071258Z	shellbag	[Session 18] ■ Folder Viewed {1D02D5DFA3230F020400000000000B02} | CLSID\{1D02D5DFA3230F020400000000000B02} | source=registry	
2025-01-14T16:02:28.071258Z	shellbag	[Session 18] ■ Folder Viewed {D102D5DFA323C302040000000000BF02} | CLSID\{D102D5DFA323C302040000000000BF02} | source=registry	
2025-01-14T16:02:28.073260Z	shellbag	[Session 18] ■ Folder Viewed {EA6588E81C0E204E9AA6EDCD0212C87C} | CLSID\{EA6588E81C0E204E9AA6EDCD0212C87C} | source=registry	
2025-01-14T16:02:28.073260Z	shellbag	[Session 18] ■ Folder Viewed {6902D5DFA3235B020400000000005702} | CLSID\{6902D5DFA3235B020400000000005702} | source=registry	
2025-01-14T16:02:28.073260Z	shellbag	[Session 18] ■ Folder Viewed {6902D5DFA3235B020400000000005702} | CLSID\{6902D5DFA3235B020400000000005702} | source=registry	
2025-01-14T16:02:28.073260Z	shellbag	[Session 18] ■ Folder Viewed {D102D5DFA323C302040000000000BF02} | CLSID\{D102D5DFA323C302040000000000BF02} | source=registry	
2025-01-14T16:02:28.075264Z	shellbag	[Session 18] ■ Folder Viewed {4D02D5DFA3233F020400000000003B02} | CLSID\{4D02D5DFA3233F020400000000003B02} | source=registry	
2025-01-14T16:02:28.075264Z	shellbag	[Session 18] ■ Folder Viewed {4D02D5DFA3233F020400000000003B02} | CLSID\{4D02D5DFA3233F020400000000003B02} | source=registry	
2025-01-14T16:02:28.075264Z	shellbag	[Session 18] ■ Folder Viewed {1D02D5DFA3230F020400000000000B02} | CLSID\{1D02D5DFA3230F020400000000000B02} | source=registry	
2025-01-14T16:02:28.087026Z	shellbag	[Session 18] ■ Folder Viewed {40F05F6481501B109F0800AA002F954E} | CLSID\{40F05F6481501B109F0800AA002F954E} | source=registry	
2025-01-14T16:02:28.087026Z	shellbag	[Session 18] ■ Folder Viewed {8D02D5DFA3237F020400000000007B02} | CLSID\{8D02D5DFA3237F020400000000007B02} | source=registry	
2025-01-14T16:02:28.089030Z	shellbag	[Session 18] ■ Folder Viewed {665C8D01334507439B53224DE2ED1FE6} | CLSID\{665C8D01334507439B53224DE2ED1FE6} | source=registry	
2025-01-14T16:02:28.089030Z	shellbag	[Session 18] ■ Folder Viewed h | CLSID\{665C8D01334507439B53224DE2ED1FE6}\h | source=registry	
2025-01-14T16:02:28.089030Z	shellbag	[Session 18] ■ Folder Viewed {8D02D5DFA3237F020400000000007B02} | CLSID\{8D02D5DFA3237F020400000000007B02} | source=registry	
2025-01-14T16:02:28.091034Z	shellbag	[Session 18] ■ Folder Viewed {1CFFCDA87848BE43B5FDF8091C1C60D0} | CLSID\{1CFFCDA87848BE43B5FDF8091C1C60D0} | source=registry	

Time	Type	Detail	Anomaly
2025-01-14T16:02:30.094980Z	shellbag	[Session 18] ■ Folder Viewed {D1A4B4B254274041A2EB9A76D9D7CDC6} | CLSID\{D1A4B4B254274041A2EB9A76D9D7CDC6} | source=registry	

Session 19 — 2 event(s)

Time	Type	Detail	Anomaly
2025-01-14T22:51:17.446480Z	lnk	[Session 19] ■ Shortcut / LNK Bluetooth File Transfer.LNK | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\SendTo\Bluetooth File Transfer.LNK | target=C:\Windows\System32\fsquirt.exe | source=pylnk3	
2025-01-14T22:51:39.837562Z	lnk	[Session 19] ■ Shortcut / LNK Fax Recipient.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\SendTo\Fax Recipient.lnk | target=C:\Windows\System32\WFS.exe | source=pylnk3	

Session 20 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T08:56:23.057078Z	shellbag	[Session 20] ■ Folder Viewed -1.0.0.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\-1.0.0.zip | source=registry	

Session 21 — 4 event(s)

Time	Type	Detail	Anomaly
2025-01-19T09:32:20.929070Z	shellbag	[Session 21] ■ Folder Viewed p | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\p | source=registry	
2025-01-19T09:32:50.298842Z	shellbag	[Session 21] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-01-19T09:32:56.410956Z	shellbag	[Session 21] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\l | source=registry	
2025-01-19T09:32:56.410956Z	shellbag	[Session 21] ■ Folder Viewed ementation | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\l\ementation | source=registry	

Session 22 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T10:09:18.307686Z	shellbag	[Session 22] ■ Folder Viewed isc_medium.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\isc_medium.zip | source=registry	

Session 23 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T10:27:22.859030Z	shellbag	[Session 23] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\isc_medium\> | source=registry	

Session 24 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T10:36:57.441396Z	shellbag	[Session 24] ■ Folder Viewed ip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\isc_medium\ip | source=registry	

Session 25 — 2 event(s)

Time	Type	Detail	Anomaly
2025-01-19T10:45:29.479808Z	shellbag	[Session 25] ■ Folder Viewed allenge.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\allenge.zip | source=registry	
2025-01-19T10:45:38.427316Z	shellbag	[Session 25] ■ Folder Viewed allenge | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\allenge | source=registry	

Session 26 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T10:49:01.176410Z	shellbag	[Session 26] ■ Folder Viewed isc_medium | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\isc_medium | source=registry	

Session 27 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T11:01:49.483952Z	shellbag	[Session 27] ■ Folder Viewed own | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\own | source=registry	

Session 28 — 2 event(s)

Time	Type	Detail	Anomaly
2025-01-19T11:12:55.255944Z	shellbag	[Session 28] ■ Folder Viewed et_Letter.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\et_Letter.zip | source=registry	
2025-01-19T11:13:04.150590Z	shellbag	[Session 28] ■ Folder Viewed et_Letter | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\et_Letter | source=registry	

Session 29 — 2 event(s)

Time	Type	Detail	Anomaly
2025-01-19T11:54:12.558506Z	shellbag	[Session 29] ■ Folder Viewed ight | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ight | source=registry	
2025-01-19T11:54:12.558506Z	shellbag	[Session 29] ■ Folder Viewed ight | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ight\ight | source=registry	

Session 30 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T12:11:01.196370Z	shellbag	[Session 30] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\ | source=registry	

Session 31 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-19T16:49:43.751024Z	lnk	[Session 31] ■ Shortcut / LNK Install RELEASE (Ubuntu).lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Ubuntu\Install RELEASE (Ubuntu).lnk | target=C:\Program Files\WSL\wslg.exe | source=pylnk3	

Session 32 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-23T05:34:17.828176Z	shellbag	[Session 32] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \@ | source=registry	

Session 33 — 1 event(s)

Time	Type	Detail	Anomaly
2025-01-23T06:53:56.914232Z	shellbag	[Session 33] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@ | source=registry	

Session 34 — 3 event(s)

Time	Type	Detail	Anomaly
2025-01-31T07:08:04.128420Z	shellbag	[Session 34] ■ Folder Viewed omcat-9.0.98-windows-x64.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\omcat-9.0.98-windows-x64.zip | source=registry	
2025-01-31T07:08:51.026040Z	shellbag	[Session 34] ■ Folder Viewed omcat-9.0.98-windows-x64 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\omcat-9.0.98-windows-x64 | source=registry	
2025-01-31T07:08:51.026040Z	shellbag	[Session 34] ■ Folder Viewed omcat-9.0.98 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\omcat-9.0.98-windows-x64\omcat-9.0.98 | source=registry	

Session 35 — 6 event(s)

Time	Type	Detail	Anomaly
2025-01-31T09:54:44.239739Z	prefetch	[Session 35] ■ Executed Program (runs: 7) DLLHOST.EXE-FE8CB7B6.pf | C:/Windows/Prefetch\DLLHOST.EXE-FE8CB7B6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=fe8cb7b6, files_count=91, volumes_count=1	
2025-01-31T09:54:44.239739Z	prefetch	[Session 35] ■ Executed Program (runs: 7) DLLHOST.EXE-FE8CB7B6.pf | C:/Windows/Prefetch\DLLHOST.EXE-FE8CB7B6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=fe8cb7b6, files_count=91, volumes_count=1	
2025-01-31T09:54:44.239739Z	prefetch	[Session 35] ■ Executed Program (runs: 7) DLLHOST.EXE-FE8CB7B6.pf | C:/Windows/Prefetch\DLLHOST.EXE-FE8CB7B6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=fe8cb7b6, files_count=91, volumes_count=1	
2025-01-31T09:56:07.715772Z	prefetch	[Session 35] ■ Executed Program (runs: 3) A~NSISU_.EXE-98418A8C.pf | C:/Windows/Prefetch\A~NSISU_.EXE-98418A8C.pf | exe=A~NSISU_.EXE | source=local:poor_billionaire, pref_hash=98418a8c, files_count=67, volumes_count=1	
2025-01-31T09:56:07.715772Z	prefetch	[Session 35] ■ Executed Program (runs: 3) A~NSISU_.EXE-98418A8C.pf | C:/Windows/Prefetch\A~NSISU_.EXE-98418A8C.pf | exe=A~NSISU_.EXE | source=local:poor_billionaire, pref_hash=98418a8c, files_count=67, volumes_count=1	
2025-01-31T09:56:07.715772Z	prefetch	[Session 35] ■ Executed Program (runs: 3) A~NSISU_.EXE-98418A8C.pf | C:/Windows/Prefetch\A~NSISU_.EXE-98418A8C.pf | exe=A~NSISU_.EXE | source=local:poor_billionaire, pref_hash=98418a8c, files_count=67, volumes_count=1	

Session 36 — 3 event(s)

Time	Type	Detail	Anomaly
2025-02-06T07:16:42.122901Z	prefetch	[Session 36] ■ Executed Program (runs: 7) COPILOTNATIVE.EXE-383D3870.pf | C:/Windows/Prefetch\COPILOTNATIVE.EXE-383D3870.pf | exe=COPILOTNATIVE.EXE | source=local:poor_billionaire, pref_hash=383d3870, files_count=232, volumes_count=1	
2025-02-06T07:16:42.122901Z	prefetch	[Session 36] ■ Executed Program (runs: 7) COPILOTNATIVE.EXE-383D3870.pf | C:/Windows/Prefetch\COPILOTNATIVE.EXE-383D3870.pf | exe=COPILOTNATIVE.EXE | source=local:poor_billionaire, pref_hash=383d3870, files_count=232, volumes_count=1	
2025-02-06T07:16:42.122901Z	prefetch	[Session 36] ■ Executed Program (runs: 7) COPILOTNATIVE.EXE-383D3870.pf | C:/Windows/Prefetch\COPILOTNATIVE.EXE-383D3870.pf | exe=COPILOTNATIVE.EXE | source=local:poor_billionaire, pref_hash=383d3870, files_count=232, volumes_count=1	

Session 37 — 2 event(s)

Time	Type	Detail	Anomaly
2025-02-10T18:29:49.084974Z	shellbag	[Session 37] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-02-10T18:29:49.084974Z	shellbag	[Session 37] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \■ | source=registry	

Session 38 — 2 event(s)

Time	Type	Detail	Anomaly
2025-03-09T07:49:06.395618Z	shellbag	[Session 38] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	
2025-03-09T07:49:17.543918Z	shellbag	[Session 38] ■ Folder Viewed in | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er\in | source=registry	

Session 39 — 1 event(s)

Time	Type	Detail	Anomaly
2025-03-09T07:57:48.500412Z	shellbag	[Session 39] ■ Folder Viewed in.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er\in.zip | source=registry	

Session 40 — 2 event(s)

Time	Type	Detail	Anomaly
2025-03-09T08:05:18.005390Z	shellbag	[Session 40] ■ Folder Viewed _release | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er_release | source=registry	
2025-03-09T08:05:18.005390Z	shellbag	[Session 40] ■ Folder Viewed _release | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er_release_release | source=registry	

Session 41 — 1 event(s)

Time	Type	Detail	Anomaly
2025-03-09T08:10:07.792706Z	shellbag	[Session 41] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er | source=registry	

Session 42 — 2 event(s)

Time	Type	Detail	Anomaly
2025-03-09T08:12:16.579384Z	shellbag	[Session 42] ■ Folder Viewed _release.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er_release.zip | source=registry	
2025-03-09T08:12:16.580768Z	shellbag	[Session 42] ■ Folder Viewed {E04FD020000000000000000000000000} | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■\er_release.zip\CLSID\{E04FD020000000000000000000000000} | source=registry	

Session 43 — 3 event(s)

Time	Type	Detail	Anomaly
2025-03-12T09:31:09.916672Z	prefetch	[Session 43] ■ Executed Program (runs: 3) DLLHOST.EXE-98FFCD07.pf | C:/Windows/Prefetch\DLLHOST.EXE-98FFCD07.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=98ffcd07, files_count=64, volumes_count=1	
2025-03-12T09:31:09.916672Z	prefetch	[Session 43] ■ Executed Program (runs: 3) DLLHOST.EXE-98FFCD07.pf | C:/Windows/Prefetch\DLLHOST.EXE-98FFCD07.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=98ffcd07, files_count=64, volumes_count=1	
2025-03-12T09:31:09.916672Z	prefetch	[Session 43] ■ Executed Program (runs: 3) DLLHOST.EXE-98FFCD07.pf | C:/Windows/Prefetch\DLLHOST.EXE-98FFCD07.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=98ffcd07, files_count=64, volumes_count=1	

Session 44 — 2 event(s)

Time	Type	Detail	Anomaly
2025-03-12T09:33:27.843676Z	shellbag	[Session 44] ■ Folder Viewed omcat-11.0.5 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\omcat-11.0.5 | source=registry	
2025-03-12T09:33:27.843676Z	shellbag	[Session 44] ■ Folder Viewed omcat-11.0.5 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\omcat-11.0.5\omcat-11.0.5 | source=registry	

Session 45 — 1 event(s)

Time	Type	Detail	Anomaly
2025-03-25T13:30:05.718592Z	shellbag	[Session 45] ■ Folder Viewed {05398E082303024B98265D99428E115F} | CLSID\{05398E082303024B98265D99428E115F} | source=registry	

Session 46 — 2 event(s)

Time	Type	Detail	Anomaly
2025-04-15T07:55:47.212010Z	shellbag	[Session 46] ■ Folder Viewed {922B16D365937A46956B92703ACA08AF} | CLSID\{922B16D365937A46956B92703ACA08AF} | source=registry	
2025-04-15T07:56:45.402566Z	shellbag	[Session 46] ■ Folder Viewed | CLSID\{922B16D365937A46956B92703ACA08AF}\ | source=registry	

Session 47 — 1 event(s)

Time	Type	Detail	Anomaly
2025-04-15T08:27:19.793690Z	lnk	[Session 47] ■ Shortcut / LNK MongoDBCompass.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\MongoDB Inc\MongoDBCompass.lnk | target=C:\Users\mukul\AppData\Local\MongoDBCompass\MongoDBCompass.exe | source=pylnk3	

Session 48 — 1 event(s)

Time	Type	Detail	Anomaly
2025-04-16T07:08:48.015998Z	shellbag	[Session 48] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\■ | source=registry	

Session 49 — 5 event(s)

Time	Type	Detail	Anomaly
2025-04-16T07:18:02.534212Z	shellbag	[Session 49] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@ | source=registry	
2025-04-16T07:18:02.534212Z	shellbag	[Session 49] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\ | source=registry	
2025-04-16T07:18:09.675134Z	shellbag	[Session 49] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \> | source=registry	
2025-04-16T07:18:09.675134Z	shellbag	[Session 49] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \>\ | source=registry	
2025-04-16T07:18:33.551206Z	shellbag	[Session 49] ■ Folder Viewed | CLSID\{2F0010B7A6F519002F453A5C00000000}\ | source=registry	

Session 50 — 1 event(s)

Time	Type	Detail	Anomaly
2025-04-28T21:35:49.345178Z	shellbag	[Session 50] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\> | source=registry	

Session 51 — 4 event(s)

Time	Type	Detail	Anomaly
2025-05-04T21:46:44.712818Z	shellbag	[Session 51] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-05-04T21:46:44.712818Z	shellbag	[Session 51] ■ Folder Viewed ication2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ication2 | source=registry	
2025-05-04T21:46:52.309910Z	shellbag	[Session 51] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■ | source=registry	
2025-05-04T21:46:52.309910Z	shellbag	[Session 51] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \■\■ | source=registry	

Session 52 — 2 event(s)

Time	Type	Detail	Anomaly
2025-05-04T22:00:08.537486Z	shellbag	[Session 52] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\> | source=registry	
2025-05-04T22:00:08.537486Z	shellbag	[Session 52] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\>\ | source=registry	

Session 53 — 2 event(s)

Time	Type	Detail	Anomaly
2025-05-07T04:45:11.086402Z	shellbag	[Session 53] ■ Folder Viewed {2F0010B7A6F519002F463A5C00000000} | CLSID\{2F0010B7A6F519002F463A5C00000000} | source=registry	
2025-05-07T04:45:11.086402Z	shellbag	[Session 53] ■ Folder Viewed ■ | CLSID\{2F0010B7A6F519002F463A5C00000000}\■ | source=registry	

Session 54 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-07T04:47:55.255084Z	shellbag	[Session 54] ■ Folder Viewed do-app | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\do-app | source=registry	

Session 55 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-07T05:20:10.623300Z	shellbag	[Session 55] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \>\■ | source=registry	

Session 56 — 2 event(s)

Time	Type	Detail	Anomaly
2025-05-12T13:25:54.271126Z	shellbag	[Session 56] ■ Folder Viewed C■■t■Y^Hg■3(<mx5uI■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\<■■ 1■■■■■■■■■■■■■l■■■■■■■■■■■N■■■■■R■e■d■m■i■ ■6■■■\■\■?■\■u■s■b■#■v■i■d■_■2■7■1■7■&■p■i■d■_■f■f■4■0■#■4■8■a■c■c■6■d■6■7■d■2■9■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■ ■G■{?!■■■■&C&F+sm/ ■■■ ■■■■■■■R■e■d■m■i■ ■6■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5uI■v ■ | source=registry	
2025-05-12T13:26:12.247356Z	shellbag	[Session 56] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \er | source=registry	

Session 57 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-12T15:08:57.503496Z	shellbag	[Session 57] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \er | source=registry	

Session 58 — 2 event(s)

Time	Type	Detail	Anomaly
2025-05-12T15:11:10.095556Z	shellbag	[Session 58] ■ Folder Viewed .pdf | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \.pdf | source=registry	
2025-05-12T15:12:53.043882Z	shellbag	[Session 58] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	

Session 59 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-13T08:15:32.836056Z	shellbag	[Session 59] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \er | source=registry	

Session 60 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-13T08:17:58.394160Z	shellbag	[Session 60] ■ Folder Viewed irt | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \irt | source=registry	

Session 61 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-14T08:30:06.561202Z	shellbag	[Session 61] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ \■ | source=registry	

Session 62 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-14T09:49:47.270186Z	shellbag	[Session 62] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \@ | source=registry	

Session 63 — 3 event(s)

Time	Type	Detail	Anomaly
2025-05-15T12:16:27.617120Z	shellbag	[Session 63] ■ Folder Viewed Studio | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \Studio | source=registry	
2025-05-15T12:16:29.029204Z	shellbag	[Session 63] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \Studio\■ | source=registry	
2025-05-15T12:16:29.029204Z	shellbag	[Session 63] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \Studio\■\■ | source=registry	

Session 64 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-15T17:34:21.837690Z	shellbag	[Session 64] ■ Folder Viewed p | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\p | source=registry	

Session 65 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-15T18:38:15.378844Z	shellbag	[Session 65] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	

Session 66 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-15T19:27:14.438152Z	shellbag	[Session 66] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ \ | source=registry	

Session 67 — 2 event(s)

Time	Type	Detail	Anomaly
2025-05-15T19:33:55.947992Z	shellbag	[Session 67] ■ Folder Viewed nment | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment | source=registry	
2025-05-15T19:33:55.947992Z	shellbag	[Session 67] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \nment\@ | source=registry	

Session 68 — 6 event(s)

Time	Type	Detail	Anomaly
2025-05-15T19:36:35.223120Z	shellbag	[Session 68] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\@ | source=registry	
2025-05-15T19:36:40.853126Z	shellbag	[Session 68] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d\■ | source=registry	
2025-05-15T19:36:46.996210Z	shellbag	[Session 68] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d\> | source=registry	
2025-05-15T19:38:34.469882Z	shellbag	[Session 68] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d\ | source=registry	
2025-05-15T19:38:51.863828Z	shellbag	[Session 68] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d\■ | source=registry	
2025-05-15T19:38:51.870024Z	shellbag	[Session 68] ■ Folder Viewed ch SO1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d\■\ch SO1 | source=registry	

Session 69 — 1 event(s)

Time	Type	Detail	Anomaly
2025-05-16T11:03:14.116000Z	recycle_i	[Session 69] ■ Recycle Bin (deleted file) $IX69D3U.docx \| C:/$Recycle.Bin\S-1-5-21-509071697-2027520391-1498176977-1001\$IX69D3U.docx	

Session 70 — 2 event(s)

Time	Type	Detail	Anomaly
2025-06-02T10:42:06.043000Z	recycle_i	[Session 70] ■ Recycle Bin (deleted file) $IEBQBC7.mp4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IEBQBC7.mp4	
2025-06-02T10:42:06.043000Z	recycle_i	[Session 70] ■ Recycle Bin (deleted file) $IEBQBC7.mp4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IEBQBC7.mp4	

Session 71 — 1 event(s)

Time	Type	Detail	Anomaly
2025-06-11T04:43:06.733076Z	shellbag	[Session 71] ■ Folder Viewed _-Zip526 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:_-Zip526 | source=registry	

Session 72 — 2 event(s)

Time	Type	Detail	Anomaly
2025-06-11T04:46:39.538492Z	shellbag	[Session 72] ■ Folder Viewed _-Zip627 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:_-Zip627 | source=registry	
2025-06-11T04:46:39.538492Z	shellbag	[Session 72] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:_-Zip627\ | source=registry	

Session 73 — 2 event(s)

Time	Type	Detail	Anomaly
2025-06-12T06:13:59.880170Z	shellbag	[Session 73] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-06-12T06:13:59.880170Z	shellbag	[Session 73] ■ Folder Viewed _-Zip526 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ _-Zip526 | source=registry	

Session 74 — 3 event(s)

Time	Type	Detail	Anomaly
2025-06-13T06:24:30.246674Z	shellbag	[Session 74] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-06-13T06:25:59.286884Z	shellbag	[Session 74] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	
2025-06-13T06:26:46.971938Z	shellbag	[Session 74] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	

Session 75 — 1 event(s)

Time	Type	Detail	Anomaly
2025-06-13T07:26:52.393516Z	shellbag	[Session 75] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	

Session 76 — 3 event(s)

Time	Type	Detail	Anomaly
2025-06-22T09:22:48.526526Z	prefetch	[Session 76] ■ Executed Program (runs: 7) DLLHOST.EXE-3D55DAD9.pf | C:/Windows/Prefetch\DLLHOST.EXE-3D55DAD9.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3d55dad9, files_count=58, volumes_count=1	
2025-06-22T09:22:48.526526Z	prefetch	[Session 76] ■ Executed Program (runs: 7) DLLHOST.EXE-3D55DAD9.pf | C:/Windows/Prefetch\DLLHOST.EXE-3D55DAD9.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3d55dad9, files_count=58, volumes_count=1	
2025-06-22T09:22:48.526526Z	prefetch	[Session 76] ■ Executed Program (runs: 7) DLLHOST.EXE-3D55DAD9.pf | C:/Windows/Prefetch\DLLHOST.EXE-3D55DAD9.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3d55dad9, files_count=58, volumes_count=1	

Session 77 — 1 event(s)

Time	Type	Detail	Anomaly
2025-06-23T15:19:59.887568Z	shellbag	[Session 77] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d | source=registry	

Session 78 — 1 event(s)

Time	Type	Detail	Anomaly
2025-08-14T09:18:53.233248Z	lnk	[Session 78] ■ Shortcut / LNK Postman.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Postman\Postman.lnk | target=C:\Users\mukul\AppData\Local\Postman\Postman.exe | source=pylnk3	

Session 79 — 1 event(s)

Time	Type	Detail	Anomaly
2025-09-02T07:42:59.341038Z	shellbag	[Session 79] ■ Folder Viewed ip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ip | source=registry	

Session 80 — 1 event(s)

Time	Type	Detail	Anomaly
2025-09-02T09:21:01.371860Z	shellbag	[Session 80] ■ Folder Viewed Mobile Forensics-20250902T092023Z-1-001 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Mobile Forensics-20250902T092023Z-1-001 | source=registry	

Session 81 — 3 event(s)

Time	Type	Detail	Anomaly
2025-09-02T09:30:44.042565Z	prefetch	[Session 81] ■ Executed Program (runs: 3) ADENCRYPT_GUI.EXE-D929D9E3.pf | C:/Windows/Prefetch\ADENCRYPT_GUI.EXE-D929D9E3.pf | exe=ADENCRYPT_GUI.EXE | source=local:poor_billionaire, pref_hash=d929d9e3, files_count=179, volumes_count=1	
2025-09-02T09:30:44.042565Z	prefetch	[Session 81] ■ Executed Program (runs: 3) ADENCRYPT_GUI.EXE-D929D9E3.pf | C:/Windows/Prefetch\ADENCRYPT_GUI.EXE-D929D9E3.pf | exe=ADENCRYPT_GUI.EXE | source=local:poor_billionaire, pref_hash=d929d9e3, files_count=179, volumes_count=1	
2025-09-02T09:30:44.042565Z	prefetch	[Session 81] ■ Executed Program (runs: 3) ADENCRYPT_GUI.EXE-D929D9E3.pf | C:/Windows/Prefetch\ADENCRYPT_GUI.EXE-D929D9E3.pf | exe=ADENCRYPT_GUI.EXE | source=local:poor_billionaire, pref_hash=d929d9e3, files_count=179, volumes_count=1	

Session 82 — 3 event(s)

Time	Type	Detail	Anomaly
2025-09-02T09:34:32.737498Z	shellbag	[Session 82] ■ Folder Viewed Mobile Forensics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Mobile Forensics-20250902T092023Z-1-001\Mobile Forensics | source=registry	
2025-09-02T09:34:33.887454Z	shellbag	[Session 82] ■ Folder Viewed F | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Mobile Forensics-20250902T092023Z-1-001\Mobile Forensics\F | source=registry	
2025-09-02T09:34:33.887454Z	shellbag	[Session 82] ■ Folder Viewed F | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Mobile Forensics-20250902T092023Z-1-001\Mobile Forensics\F\F | source=registry	

Session 83 — 3 event(s)

Time	Type	Detail	Anomaly
2025-09-02T10:15:23.941691Z	prefetch	[Session 83] ■ Executed Program (runs: 3) AUTOPSY64.EXE-FB77C07A.pf | C:/Windows/Prefetch\AUTOPSY64.EXE-FB77C07A.pf | exe=AUTOPSY64.EXE | source=local:poor_billionaire, pref_hash=fb77c07a, files_count=510, volumes_count=1	
2025-09-02T10:15:23.941691Z	prefetch	[Session 83] ■ Executed Program (runs: 3) AUTOPSY64.EXE-FB77C07A.pf | C:/Windows/Prefetch\AUTOPSY64.EXE-FB77C07A.pf | exe=AUTOPSY64.EXE | source=local:poor_billionaire, pref_hash=fb77c07a, files_count=510, volumes_count=1	
2025-09-02T10:15:23.941691Z	prefetch	[Session 83] ■ Executed Program (runs: 3) AUTOPSY64.EXE-FB77C07A.pf | C:/Windows/Prefetch\AUTOPSY64.EXE-FB77C07A.pf | exe=AUTOPSY64.EXE | source=local:poor_billionaire, pref_hash=fb77c07a, files_count=510, volumes_count=1	

Session 84 — 4 event(s)

Time	Type	Detail	Anomaly
2025-09-02T10:39:16.795132Z	shellbag	[Session 84] ■ Folder Viewed Reader file-20250902T103615Z-1-002.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Reader file-20250902T103615Z-1-002.zip | source=registry	
2025-09-02T10:40:57.877974Z	shellbag	[Session 84] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\> | source=registry	
2025-09-02T10:41:16.322162Z	shellbag	[Session 84] ■ Folder Viewed Reader file-20250902T103615Z-1-002 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Reader file-20250902T103615Z-1-002 | source=registry	
2025-09-02T10:41:17.320704Z	shellbag	[Session 84] ■ Folder Viewed Reader file | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\Reader file-20250902T103615Z-1-002\Reader file | source=registry	

Session 85 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-01T10:41:03.314266Z	shellbag	[Session 85] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\er | source=registry	
2025-10-01T10:41:03.314266Z	shellbag	[Session 85] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\er\er | source=registry	

Session 86 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-06T13:46:57.538544Z	shellbag	[Session 86] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	
2025-10-06T13:47:10.157108Z	shellbag	[Session 86] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Session 87 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-06T13:59:16.080516Z	prefetch	[Session 87] ■ Executed Program (runs: 7) CALCULATORAPP.EXE-562DD422.pf | C:/Windows/Prefetch\CALCULATORAPP.EXE-562DD422.pf | exe=CALCULATORAPP.EXE | source=local:poor_billionaire, pref_hash=562dd422, files_count=147, volumes_count=1	
2025-10-06T13:59:16.080516Z	prefetch	[Session 87] ■ Executed Program (runs: 7) CALCULATORAPP.EXE-562DD422.pf | C:/Windows/Prefetch\CALCULATORAPP.EXE-562DD422.pf | exe=CALCULATORAPP.EXE | source=local:poor_billionaire, pref_hash=562dd422, files_count=147, volumes_count=1	
2025-10-06T13:59:16.080516Z	prefetch	[Session 87] ■ Executed Program (runs: 7) CALCULATORAPP.EXE-562DD422.pf | C:/Windows/Prefetch\CALCULATORAPP.EXE-562DD422.pf | exe=CALCULATORAPP.EXE | source=local:poor_billionaire, pref_hash=562dd422, files_count=147, volumes_count=1	

Session 88 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-06T20:28:23.064370Z	shellbag	[Session 88] ■ Folder Viewed sExplorer.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\sExplorer.zip | source=registry	
2025-10-06T20:28:44.222856Z	shellbag	[Session 88] ■ Folder Viewed sExplorer | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\sExplorer | source=registry	

Session 89 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-06T20:33:37.845660Z	shellbag	[Session 89] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\ | source=registry	

Session 90 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-06T20:59:38.170196Z	shellbag	[Session 90] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\sExplorer\sExplorer\ | source=registry	

Session 91 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-10T03:55:47.993396Z	shellbag	[Session 91] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Session 92 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-12T22:32:50.651618Z	shellbag	[Session 92] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	

Session 93 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-13T20:51:43.563734Z	shellbag	[Session 93] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ \ | source=registry	

Session 94 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-13T21:00:48.012926Z	shellbag	[Session 94] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	

Session 95 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-15T17:28:52.179316Z	shellbag	[Session 95] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Session 96 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-15T19:22:47.689678Z	shellbag	[Session 96] ■ Folder Viewed {ABA36FF8D270C74F9C99FCBF05467F3A} | CLSID\{ABA36FF8D270C74F9C99FCBF05467F3A} | source=registry	
2025-10-15T19:22:47.689678Z	shellbag	[Session 96] ■ Folder Viewed @ | CLSID\{ABA36FF8D270C74F9C99FCBF05467F3A}\@ | source=registry	

Session 97 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-16T17:22:20.799852Z	shellbag	[Session 97] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \> | source=registry	

Session 98 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-18T19:19:24.139156Z	shellbag	[Session 98] ■ Folder Viewed C■■t■Y^Hg■3(<mx5ul■v ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\f■■ 1■■■■■■■■■■■■■■■■■■■■■■■■l■■■■■R■e■d■m■i■ ■N■o■t■e■ ■9■ ■P■r■o■ ■M■a■x■■■\■\■?■\■u■s■b■#■v■i■d■_■2■7■1■7■&■p■i■d■_■f■f■4■0■#■e■2■c■8■f■7■2■#■{■6■a■c■2■7■8■7■8■-■a■6■f■a■-■4■1■5■5■-■b■a■8■5■-■f■9■8■f■4■9■1■d■4■f■3■3■}■■■ ■■■■■■G■{?!■■■■&C&F+sm/ ■■■ ■■■*■■■R■e■d■m■i■ ■N■o■t■e■ ■9■ ■P■r■o■ ■M■a■x■■■-■O ■■■■H■■■kF■6CM+\C■■t■Y^Hg■3(<mx5ul■v ■ | source=registry	

Session 99 — 5 event(s)

Time	Type	Detail	Anomaly
2025-10-21T01:00:35.389485Z	prefetch	[Session 99] ■ Executed Program (runs: 7) DLLHOST.EXE-3F9B2B1D.pf | C:/Windows/Prefetch\DLLHOST.EXE-3F9B2B1D.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3f9b2b1d, files_count=46, volumes_count=1	
2025-10-21T01:00:35.389485Z	prefetch	[Session 99] ■ Executed Program (runs: 7) DLLHOST.EXE-3F9B2B1D.pf | C:/Windows/Prefetch\DLLHOST.EXE-3F9B2B1D.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3f9b2b1d, files_count=46, volumes_count=1	
2025-10-21T01:00:35.389485Z	prefetch	[Session 99] ■ Executed Program (runs: 7) DLLHOST.EXE-3F9B2B1D.pf | C:/Windows/Prefetch\DLLHOST.EXE-3F9B2B1D.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=3f9b2b1d, files_count=46, volumes_count=1	
2025-10-21T01:00:43.557250Z	shellbag	[Session 99] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	
2025-10-21T01:00:43.557250Z	shellbag	[Session 99] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ | source=registry	

Session 100 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T16:59:53.986162Z	shellbag	[Session 100] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ | source=registry	

Session 101 — 6 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:02:44.191176Z	shellbag	[Session 101] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\> | source=registry	
2025-10-30T17:03:51.013312Z	shellbag	[Session 101] ■ Folder Viewed HUNT__VM.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__VM.zip | source=registry	
2025-10-30T17:04:33.843214Z	shellbag	[Session 101] ■ Folder Viewed HUNT__VM | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__VM | source=registry	
2025-10-30T17:04:36.852684Z	shellbag	[Session 101] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__VM\■\■ | source=registry	
2025-10-30T17:05:38.842196Z	shellbag	[Session 101] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__VM\■ | source=registry	
2025-10-30T17:05:38.842196Z	shellbag	[Session 101] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__VM\■\■ | source=registry	

Session 102 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:12:43.251456Z	shellbag	[Session 102] ■ Folder Viewed HUNT__room | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__room | source=registry	

Session 103 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:15:02.641636Z	shellbag	[Session 103] ■ Folder Viewed llege Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \llege Girl | source=registry	
2025-10-30T17:15:08.057736Z	shellbag	[Session 103] ■ Folder Viewed HUNT__10cli | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__10cli | source=registry	

Session 104 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:22:02.433046Z	shellbag	[Session 104] ■ Folder Viewed w_MmsHunt_Com | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \w MmsHunt\w_MmsHunt_Com | source=registry	
2025-10-30T17:22:02.434054Z	shellbag	[Session 104] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \w MmsHunt\w_MmsHunt_Com\ | source=registry	

Session 105 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:29:26.074946Z	shellbag	[Session 105] ■ Folder Viewed shevade 1.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ shevade 1.zip | source=registry	
2025-10-30T17:30:04.294752Z	shellbag	[Session 105] ■ Folder Viewed shevade 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ shevad\ shevade 1 | source=registry	
2025-10-30T17:30:04.295754Z	shellbag	[Session 105] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ shevad\ shevade 1\> | source=registry	

Session 106 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:37:48.814388Z	shellbag	[Session 106] ■ Folder Viewed HUNT__SxyGg.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__SxyGg.zip | source=registry	

Session 107 — 4 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:41:31.673464Z	shellbag	[Session 107] ■ Folder Viewed Town__UpdateeMP.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__UpdateeMP.zip | source=registry	
2025-10-30T17:41:42.092198Z	shellbag	[Session 107] ■ Folder Viewed Town__UpdateeMP | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__UpdateeMP | source=registry	
2025-10-30T17:41:57.481320Z	shellbag	[Session 107] ■ Folder Viewed MP | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__UpdateeMP\MP | source=registry	
2025-10-30T17:41:57.481320Z	shellbag	[Session 107] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__UpdateeMP\MP\> | source=registry	

Session 108 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-30T17:47:12.560040Z	shellbag	[Session 108] ■ Folder Viewed Dose__MlluGirlP | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__MlluGirlP | source=registry	
2025-10-30T17:48:28.511676Z	shellbag	[Session 108] ■ Folder Viewed llege Lesbian | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \llege Lesbian | source=registry	
2025-10-30T17:48:28.511676Z	shellbag	[Session 108] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \llege Lesbian\> | source=registry	

Session 109 — 1 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-10-30T17:53:59.471024Z</td><td>shellbag</td><td>[Session 109] ■ Folder Viewed ther Changing Clothes | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ther Changing Clothes | source=registry</td><td></td></tr>
</table>

Session 110 — 4 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-10-30T18:05:01.492812Z</td><td>shellbag</td><td>[Session 110] ■ Folder Viewed _720p | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ _720p | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:05:23.298310Z</td><td>shellbag</td><td>[Session 110] ■ Folder Viewed Dose.org_3BFF | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose.org_3BFF | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:05:23.298310Z</td><td>shellbag</td><td>[Session 110] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose.org_3BFF\ | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:06:34.021386Z</td><td>shellbag</td><td>[Session 110] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ | source=registry</td><td></td></tr>
</table>

Session 111 — 10 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-10-30T18:19:54.197000Z</td><td>recycle_i</td><td>[Session 111] ■ Recycle Bin (deleted file) $I9QL23J.mp4 | D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I9QL23J.mp4</td><td></td></tr>
<tr><td>2025-10-30T18:19:54.197000Z</td><td>recycle_i</td><td>[Session 111] ■ Recycle Bin (deleted file) $I9QL23J.mp4 | D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I9QL23J.mp4</td><td></td></tr>
<tr><td>2025-10-30T18:19:54.199000Z</td><td>recycle_i</td><td>[Session 111] ■ Recycle Bin (deleted file) $IYKWQBP.mp4 | D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IYKWQBP.mp4</td><td></td></tr>
<tr><td>2025-10-30T18:19:54.199000Z</td><td>recycle_i</td><td>[Session 111] ■ Recycle Bin (deleted file) $IYKWQBP.mp4 | D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IYKWQBP.mp4</td><td></td></tr>
<tr><td>2025-10-30T18:20:43.618550Z</td><td>shellbag</td><td>[Session 111] ■ Folder Viewed 15254 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \15254 | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:21:37.245322Z</td><td>shellbag</td><td>[Session 111] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:22:26.831690Z</td><td>shellbag</td><td>[Session 111] ■ Folder Viewed Dose__Updatee2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__Updatee2 | source=registry</td><td></td></tr>
<tr><td>2025-10-30T18:23:08.513504Z</td><td>shellbag</td><td>[Session 111] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \> | source=registry</td><td></td></tr>
</table>

Time	Type	Detail	Anomaly
2025-10-30T18:24:00.768690Z	shellbag	[Session 111] ■ Folder Viewed Dose__hunterkiss | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__hunterkiss | source=registry	
2025-10-30T18:24:00.768690Z	shellbag	[Session 111] ■ Folder Viewed iss | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__hunterkiss\iss | source=registry	

Session 112 — 4 event(s)

Time	Type	Detail	Anomaly
2025-10-30T18:33:52.523340Z	shellbag	[Session 112] ■ Folder Viewed Dose__15 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__15 | source=registry	
2025-10-30T18:35:43.691966Z	shellbag	[Session 112] ■ Folder Viewed Dose__Malluvalentinesoutdoorupdate12clips | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__Malluvalentinesoutdoorupdate12clips | source=registry	
2025-10-30T18:35:54.332954Z	shellbag	[Session 112] ■ Folder Viewed Dose__9clips | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__9clips | source=registry	
2025-10-30T18:36:26.333752Z	shellbag	[Session 112] ■ Folder Viewed ni | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ni | source=registry	

Session 113 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T18:43:54.045796Z	shellbag	[Session 113] ■ Folder Viewed st | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \st | source=registry	

Session 114 — 14 event(s)

Time	Type	Detail	Anomaly
2025-10-30T18:49:55.242320Z	shellbag	[Session 114] ■ Folder Viewed Town__MalluLovers | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__MalluLovers | source=registry	
2025-10-30T18:49:55.242320Z	shellbag	[Session 114] ■ Folder Viewed ers | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Town__MalluLovers\ers | source=registry	
2025-10-30T18:50:47.810260Z	shellbag	[Session 114] ■ Folder Viewed Dose__BustyPakiHootGirlFullFukVideosPics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BustyPakiHootGirlFullFukVideosPics | source=registry	
2025-10-30T18:51:41.027640Z	shellbag	[Session 114] ■ Folder Viewed ki Hoot Girl Full Fuk Videos & Pics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BustyPakiHootGirlFullFukVideosPics\ki Hoot Girl Full Fuk Videos & Pics | source=registry	
2025-10-30T18:51:41.029630Z	shellbag	[Session 114] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BustyPakiHootGirlFullFukVideosPics\ki Hoot Girl Full Fuk Videos & Pics\■ | source=registry	
2025-10-30T18:52:17.658806Z	shellbag	[Session 114] ■ Folder Viewed ersia | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ersia | source=registry	
2025-10-30T18:52:18.546648Z	shellbag	[Session 114] ■ Folder Viewed persia | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ersia\persia | source=registry	
2025-10-30T18:52:18.546648Z	shellbag	[Session 114] ■ Folder Viewed persia(Frozen) | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ersia\persia\persia(Frozen) | source=registry	
2025-10-30T18:53:14.683756Z	shellbag	[Session 114] ■ Folder Viewed Dose__BeautyqueenPics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BeautyqueenPics | source=registry	
2025-10-30T18:53:14.683756Z	shellbag	[Session 114] ■ Folder Viewed eenPics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BeautyqueenPics\eenPics | source=registry	
2025-10-30T18:53:36.595002Z	shellbag	[Session 114] ■ Folder Viewed Dose__BeautyqueenVideos | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__BeautyqueenVideos | source=registry	
2025-10-30T18:54:04.143714Z	shellbag	[Session 114] ■ Folder Viewed eenPics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ueen\eenPics | source=registry	
2025-10-30T18:54:09.390088Z	shellbag	[Session 114] ■ Folder Viewed eenVideos | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ueen\eenVideos | source=registry	

Time	Type	Detail	Anomaly
2025-10-30T18:54:37.851092Z	shellbag	[Session 114] ■ Folder Viewed ueen | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ueen | source=registry	

Session 115 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T18:59:29.224234Z	shellbag	[Session 115] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \d | source=registry	

Session 116 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:04:11.734794Z	shellbag	[Session 116] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \■ | source=registry	

Session 117 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:12:50.391126Z	shellbag	[Session 117] ■ Folder Viewed H COLLECTION 00846 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \H COLLECTION 00846 | source=registry	
2025-10-30T19:14:37.507456Z	shellbag	[Session 117] ■ Folder Viewed Dose__6397 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__6397 | source=registry	
2025-10-30T19:14:37.507456Z	shellbag	[Session 117] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__6397\ | source=registry	

Session 118 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:18:29.635106Z	shellbag	[Session 118] ■ Folder Viewed ouple | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ouple | source=registry	
2025-10-30T19:18:29.635106Z	shellbag	[Session 118] ■ Folder Viewed uple17 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ouple\uple17 | source=registry	

Session 119 — 8 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:26:28.704408Z	shellbag	[Session 119] ■ Folder Viewed tubeErumaSaaniShyniBlowjobampFullLeaks | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \tubeErumaSaaniShyniBlowjobampFullLeaks | source=registry	
2025-10-30T19:26:28.705408Z	shellbag	[Session 119] ■ Folder Viewed utube Eruma Saani Shyni Blowjob & Full Leaks | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \tubeErumaSaaniShyniBlowjobampFullLeaks\utube Eruma Saani Shyni Blowjob & Full Leaks | source=registry	
2025-10-30T19:27:51.851916Z	shellbag	[Session 119] ■ Folder Viewed Dose__Prncpal3vds | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__Prncpal3vds | source=registry	
2025-10-30T19:27:57.520884Z	shellbag	[Session 119] ■ Folder Viewed Dose__Randi4 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__Randi4 | source=registry	
2025-10-30T19:28:19.005682Z	shellbag	[Session 119] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l | source=registry	
2025-10-30T19:28:58.512864Z	shellbag	[Session 119] ■ Folder Viewed randi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \randi | source=registry	
2025-10-30T19:29:15.825000Z	recycle_i	[Session 119] ■ Recycle Bin (deleted file) $INYCWF7.mp4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$INYCWF7.mp4	

Time	Type	Detail	Anomaly
2025-10-30T19:29:15.825000Z	recycle_i	[Session 119] ■ Recycle Bin (deleted file) $INYCWF7.mp4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$INYCWF7.mp4	

Session 120 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:32:48.462974Z	shellbag	[Session 120] ■ Folder Viewed lhi party | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lhi party | source=registry	

Session 121 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:42:12.816538Z	shellbag	[Session 121] ■ Folder Viewed Dose__16VdsUpdat | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__16VdsUpdat | source=registry	
2025-10-30T19:42:12.817572Z	shellbag	[Session 121] ■ Folder Viewed 100P | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__16VdsUpdat\100P | source=registry	

Session 122 — 8 event(s)

Time	Type	Detail	Anomaly
2025-10-30T19:51:52.626652Z	shellbag	[Session 122] ■ Folder Viewed xy Young Indian Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \xy Young Indian Girl | source=registry	
2025-10-30T19:52:16.352172Z	shellbag	[Session 122] ■ Folder Viewed y Young Teen 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Young Teen 1 | source=registry	
2025-10-30T19:52:45.081534Z	shellbag	[Session 122] ■ Folder Viewed y Young Teen | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Young Teen | source=registry	
2025-10-30T19:52:45.081534Z	shellbag	[Session 122] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Young Teen\■ | source=registry	
2025-10-30T19:53:15.858088Z	shellbag	[Session 122] ■ Folder Viewed her Tution Teacher Dick | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \her Tution Teacher Dick | source=registry	
2025-10-30T19:53:15.858088Z	shellbag	[Session 122] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \her Tution Teacher Dick\@ | source=registry	
2025-10-30T19:53:25.062140Z	shellbag	[Session 122] ■ Folder Viewed her Tution Teacher Dick 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \her Tution Teacher Dick 1 | source=registry	
2025-10-30T19:53:25.062140Z	shellbag	[Session 122] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \her Tution Teacher Dick 1\@ | source=registry	

Session 123 — 7 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:02:49.043720Z	shellbag	[Session 123] ■ Folder Viewed tagram Influencer | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \tagram Influencer | source=registry	
2025-10-30T20:02:49.043720Z	shellbag	[Session 123] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \tagram Influencer\s | source=registry	
2025-10-30T20:03:23.781962Z	shellbag	[Session 123] ■ Folder Viewed DSM Couple 2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \DSM Couple 2 | source=registry	

Time	Type	Detail	Anomaly
2025-10-30T20:03:23.781962Z	shellbag	[Session 123] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \DSM Couple 2\■ | source=registry	
2025-10-30T20:03:29.810198Z	shellbag	[Session 123] ■ Folder Viewed DSM Couple | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \DSM Couple | source=registry	
2025-10-30T20:03:29.810198Z	shellbag	[Session 123] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \DSM Couple\■ | source=registry	
2025-10-30T20:03:34.928596Z	shellbag	[Session 123] ■ Folder Viewed DSM Couple 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \DSM Couple 1 | source=registry	

Session 124 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:05:41.855632Z	shellbag	[Session 124] ■ Folder Viewed persia | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \persia | source=registry	
2025-10-30T20:05:41.855632Z	shellbag	[Session 124] ■ Folder Viewed persia(Frozen) | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \persia\persia(Frozen) | source=registry	
2025-10-30T20:06:25.676634Z	shellbag	[Session 124] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Milky Body Kannada Wife\■ | source=registry	

Session 125 — 4 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:11:40.893622Z	shellbag	[Session 125] ■ Folder Viewed Babe Kriti | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Kriti | source=registry	
2025-10-30T20:11:40.893622Z	shellbag	[Session 125] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Kriti\ | source=registry	
2025-10-30T20:11:47.218724Z	shellbag	[Session 125] ■ Folder Viewed Babe Kriti1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Kriti1 | source=registry	
2025-10-30T20:11:47.218724Z	shellbag	[Session 125] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Kriti1\> | source=registry	

Session 126 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:19:02.531220Z	shellbag	[Session 126] ■ Folder Viewed ecretary | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ecretary | source=registry	

Session 127 — 5 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:32:33.529998Z	shellbag	[Session 127] ■ Folder Viewed Babe Giving Blowjob 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Giving Blowjob 1 | source=registry	
2025-10-30T20:34:17.372430Z	shellbag	[Session 127] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Giving Blowjob\> | source=registry	
2025-10-30T20:34:35.493912Z	shellbag	[Session 127] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Giving Blowjob\■ | source=registry	
2025-10-30T20:36:16.854100Z	shellbag	[Session 127] ■ Folder Viewed Babe Giving Blowjob | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Giving Blowjob | source=registry	
2025-10-30T20:36:16.854100Z	shellbag	[Session 127] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Babe Giving Blowjob\■ | source=registry	

Session 128 — 5 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:39:24.241810Z	shellbag	[Session 128] ■ Folder Viewed amer Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \amer Girl | source=registry	
2025-10-30T20:39:24.241810Z	shellbag	[Session 128] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \amer Girl\ | source=registry	

Time	Type	Detail	Anomaly
2025-10-30T20:40:12.234694Z	shellbag	[Session 128] ■ Folder Viewed Girl Muskan 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\\Girl Muskan 1 | source=registry	
2025-10-30T20:40:12.234694Z	shellbag	[Session 128] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\\Girl Muskan 1\ | source=registry	
2025-10-30T20:40:26.800488Z	shellbag	[Session 128] ■ Folder Viewed Girl Muskan 3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\\Girl Muskan 3 | source=registry	

Session 129 — 5 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:48:57.251014Z	shellbag	[Session 129] ■ Folder Viewed ing Illegal Affair.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ing Illegal Affair.zip | source=registry	
2025-10-30T20:49:11.325708Z	shellbag	[Session 129] ■ Folder Viewed napchat Babe | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \napchat Babe | source=registry	
2025-10-30T20:49:11.326688Z	shellbag	[Session 129] ■ Folder Viewed ja | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \napchat Babe\ja | source=registry	
2025-10-30T20:49:34.974976Z	shellbag	[Session 129] ■ Folder Viewed ing Illegal Affair | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ing Illegal Affair | source=registry	
2025-10-30T20:49:34.974976Z	shellbag	[Session 129] ■ Folder Viewed gwife | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ing Illegal Affair\gwife | source=registry	

Session 130 — 7 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:53:33.725170Z	shellbag	[Session 130] ■ Folder Viewed jabi Couple | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \jabi Couple | source=registry	
2025-10-30T20:53:34.507822Z	shellbag	[Session 130] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \jabi Couple\@ | source=registry	
2025-10-30T20:53:35.214992Z	shellbag	[Session 130] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \jabi Couple\@\ | source=registry	
2025-10-30T20:53:36.052666Z	shellbag	[Session 130] ■ Folder Viewed sapp | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \jabi Couple\@\ \sapp | source=registry	
2025-10-30T20:54:13.975940Z	shellbag	[Session 130] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ | source=registry	
2025-10-30T20:54:13.975940Z	shellbag	[Session 130] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ \ | source=registry	
2025-10-30T20:54:44.737912Z	shellbag	[Session 130] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ | source=registry	

Session 131 — 4 event(s)

Time	Type	Detail	Anomaly
2025-10-30T20:57:36.044514Z	shellbag	[Session 131] ■ Folder Viewed Spying on her Sister | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Spying on her Sister | source=registry	

Time	Type	Detail	Anomaly
2025-10-30T20:57:36.044514Z	shellbag	[Session 131] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Spying on her Sister\s | source=registry	
2025-10-30T20:59:26.755540Z	shellbag	[Session 131] ■ Folder Viewed d couple | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \d couple | source=registry	
2025-10-30T20:59:26.755540Z	shellbag	[Session 131] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \d couple\ | source=registry	

Session 132 — 5 event(s)

Time	Type	Detail	Anomaly
2025-10-30T21:24:33.519926Z	shellbag	[Session 132] ■ Folder Viewed ctress | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ctress | source=registry	
2025-10-30T21:25:17.464300Z	shellbag	[Session 132] ■ Folder Viewed rich girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ rich girl | source=registry	
2025-10-30T21:25:17.464300Z	shellbag	[Session 132] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ rich girl\ | source=registry	
2025-10-30T21:25:30.254004Z	shellbag	[Session 132] ■ Folder Viewed y_Teacher | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y_Teacher | source=registry	
2025-10-30T21:25:30.254004Z	shellbag	[Session 132] ■ Folder Viewed y_Teacher | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y_Teacher\y_Teacher | source=registry	

Session 133 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-30T21:28:31.525634Z	shellbag	[Session 133] ■ Folder Viewed Girl Muskan | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Girl Muskan | source=registry	
2025-10-30T21:28:31.525634Z	shellbag	[Session 133] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Girl Muskan\ | source=registry	

Session 134 — 7 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:05:19.313236Z	shellbag	[Session 134] ■ Folder Viewed e | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \e | source=registry	
2025-10-31T16:05:59.980750Z	shellbag	[Session 134] ■ Folder Viewed Lover | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Lover | source=registry	
2025-10-31T16:05:59.981754Z	shellbag	[Session 134] ■ Folder Viewed eOld+New | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Lover\eOld+New | source=registry	
2025-10-31T16:07:08.230080Z	shellbag	[Session 134] ■ Folder Viewed Secretly Recorded her Mother | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Secretly Recorded her Mother | source=registry	
2025-10-31T16:07:08.230080Z	shellbag	[Session 134] ■ Folder Viewed HUNT__OtherHousekeeper | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Secretly Recorded her Mother\HUNT__OtherHousekeeper | source=registry	
2025-10-31T16:08:44.345288Z	shellbag	[Session 134] ■ Folder Viewed e | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \e | source=registry	
2025-10-31T16:08:44.345288Z	shellbag	[Session 134] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \e\■ | source=registry	

Session 135 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:11:13.786612Z	shellbag	[Session 135] ■ Folder Viewed lhi Sexy Curvy | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lhi Sexy Curvy | source=registry	
2025-10-31T16:11:13.786612Z	shellbag	[Session 135] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lhi Sexy Curvy\■ | source=registry	

Session 136 — 4 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:13:32.784008Z	shellbag	[Session 136] ■ Folder Viewed rny Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \rny Girl | source=registry	
2025-10-31T16:13:58.141378Z	prefetch	[Session 136] ■ Executed Program (runs: 3) DEVENV.EXE-9B71354E.pf | C:/Windows/Prefetch\DEVENV.EXE-9B71354E.pf | exe=DEVENV.EXE | source=local:poor_billionaire, pref_hash=9b71354e, files_count=382, volumes_count=1	
2025-10-31T16:13:58.141378Z	prefetch	[Session 136] ■ Executed Program (runs: 3) DEVENV.EXE-9B71354E.pf | C:/Windows/Prefetch\DEVENV.EXE-9B71354E.pf | exe=DEVENV.EXE | source=local:poor_billionaire, pref_hash=9b71354e, files_count=382, volumes_count=1	
2025-10-31T16:13:58.141378Z	prefetch	[Session 136] ■ Executed Program (runs: 3) DEVENV.EXE-9B71354E.pf | C:/Windows/Prefetch\DEVENV.EXE-9B71354E.pf | exe=DEVENV.EXE | source=local:poor_billionaire, pref_hash=9b71354e, files_count=382, volumes_count=1	

Session 137 — 2 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:25:44.742898Z	shellbag	[Session 137] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \@ | source=registry	
2025-10-31T16:25:44.742898Z	shellbag	[Session 137] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \@\ | source=registry	

Session 138 — 9 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:51:59.038590Z	shellbag	[Session 138] ■ Folder Viewed ladeshi Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ladeshi Girl | source=registry	
2025-10-31T16:51:59.038590Z	shellbag	[Session 138] ■ Folder Viewed _Frozen_ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ladeshi Girl_Frozen_ | source=registry	
2025-10-31T16:52:15.445888Z	shellbag	[Session 138] ■ Folder Viewed fluencer Nidhi Joshi 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Nidhi Joshi 1 | source=registry	
2025-10-31T16:52:15.445888Z	shellbag	[Session 138] ■ Folder Viewed shi_pics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Nidhi Joshi 1\shi_pics | source=registry	
2025-10-31T16:52:32.577670Z	shellbag	[Session 138] ■ Folder Viewed shi_Vids | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Nidhi Joshi\shi_Vids | source=registry	
2025-10-31T16:52:47.952680Z	shellbag	[Session 138] ■ Folder Viewed harma | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \harma | source=registry	
2025-10-31T16:52:47.953778Z	shellbag	[Session 138] ■ Folder Viewed harma videos | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \harma\harma videos | source=registry	
2025-10-31T16:52:59.479040Z	shellbag	[Session 138] ■ Folder Viewed Drunk College Best Friends | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Drunk College Best Friends | source=registry	
2025-10-31T16:54:57.571618Z	shellbag	[Session 138] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \@ | source=registry	

Session 139 — 3 event(s)

Time	Type	Detail	Anomaly
2025-10-31T16:57:38.728052Z	shellbag	[Session 139] ■ Folder Viewed ers | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ers | source=registry	
2025-10-31T16:57:46.910506Z	shellbag	[Session 139] ■ Folder Viewed fluencer Nidhi Joshi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Nidhi Joshi | source=registry	

Time	Type	Detail	Anomaly
2025-10-31T16:57:46.910506Z	shellbag	[Session 139] ■ Folder Viewed shi_pics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Nidhi Joshi\shi_pics | source=registry	

Session 140 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-31T17:14:49.171548Z	shellbag	[Session 140] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l | source=registry	

Session 141 — 11 event(s)

Time	Type	Detail	Anomaly
2025-10-31T17:17:14.285378Z	shellbag	[Session 141] ■ Folder Viewed NDAL | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \NDAL | source=registry	
2025-10-31T17:18:03.654980Z	shellbag	[Session 141] ■ Folder Viewed Girl Siya | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Girl Siya | source=registry	
2025-10-31T17:18:09.065158Z	shellbag	[Session 141] ■ Folder Viewed Girl Siya 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ Girl Siya 1 | source=registry	
2025-10-31T17:18:31.344062Z	shellbag	[Session 141] ■ Folder Viewed lean Shaved Pink Pussy | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lean Shaved Pink Pussy | source=registry	
2025-10-31T17:18:31.344062Z	shellbag	[Session 141] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lean Shaved Pink Pussy\ | source=registry	
2025-10-31T17:18:45.078228Z	shellbag	[Session 141] ■ Folder Viewed uples Outdoor | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \uples Outdoor | source=registry	
2025-10-31T17:18:46.370540Z	shellbag	[Session 141] ■ Folder Viewed Dose__part1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \uples Outdoor\Dose__part1 | source=registry	
2025-10-31T17:18:46.370540Z	shellbag	[Session 141] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \uples Outdoor\Dose__part1\> | source=registry	
2025-10-31T17:18:57.325298Z	shellbag	[Session 141] ■ Folder Viewed uples Outdoor 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \uples Outdoor 1 | source=registry	
2025-10-31T17:18:57.325298Z	shellbag	[Session 141] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \uples Outdoor 1\> | source=registry	
2025-10-31T17:19:11.421654Z	shellbag	[Session 141] ■ Folder Viewed d Handcuffs on Windows | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \d Handcuffs on Windows | source=registry	

Session 142 — 14 event(s)

Time	Type	Detail	Anomaly
2025-10-31T18:09:37.288820Z	shellbag	[Session 142] ■ Folder Viewed llege Girl Bunk Class 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \llege Girl Bunk Class 1 | source=registry	
2025-10-31T18:09:45.414654Z	shellbag	[Session 142] ■ Folder Viewed llege Girl Bunk Class | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \llege Girl Bunk Class | source=registry	
2025-10-31T18:09:59.982950Z	shellbag	[Session 142] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \■ | source=registry	

Time	Type	Detail	Anomaly
2025-10-31T18:10:45.360298Z	shellbag	[Session 142] ■ Folder Viewed rvayi Hai | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \rvayi Hai | source=registry	
2025-10-31T18:10:49.881828Z	shellbag	[Session 142] ■ Folder Viewed rvayi Hai 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \rvayi Hai 1 | source=registry	
2025-10-31T18:11:27.970540Z	shellbag	[Session 142] ■ Folder Viewed l Prachi 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Prachi 1 | source=registry	
2025-10-31T18:11:27.970540Z	shellbag	[Session 142] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Prachi 1\ | source=registry	
2025-10-31T18:11:33.193000Z	shellbag	[Session 142] ■ Folder Viewed l Prachi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Prachi | source=registry	
2025-10-31T18:11:50.658548Z	shellbag	[Session 142] ■ Folder Viewed shi Teen Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \shi Teen Girl | source=registry	
2025-10-31T18:11:50.658548Z	shellbag	[Session 142] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \shi Teen Girl\> | source=registry	
2025-10-31T18:12:02.855708Z	shellbag	[Session 142] ■ Folder Viewed shi Teen Girl 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \shi Teen Girl 1 | source=registry	
2025-10-31T18:12:14.171120Z	shellbag	[Session 142] ■ Folder Viewed shi Teen Girl 2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \shi Teen Girl 2 | source=registry	
2025-10-31T18:12:35.257534Z	shellbag	[Session 142] ■ Folder Viewed e IT College Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \e IT College Girl | source=registry	
2025-10-31T18:12:35.257534Z	shellbag	[Session 142] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \e IT College Girl\■ | source=registry	

Session 143 — 1 event(s)

Time	Type	Detail	Anomaly
2025-10-31T18:15:20.444332Z	shellbag	[Session 143] ■ Folder Viewed ngali Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ngali Girl | source=registry	

Session 144 — 15 event(s)

Time	Type	Detail	Anomaly
2025-11-03T10:03:01.065398Z	shellbag	[Session 144] ■ Folder Viewed lTnkr | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lTnkr | source=registry	

Time	Type	Detail	Anomaly
2025-11-03T10:03:01.065398Z	shellbag	[Session 144] ■ Folder Viewed lTnkr | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lTnkr\lTnkr | source=registry	
2025-11-03T10:03:24.539316Z	shellbag	[Session 144] ■ Folder Viewed Babe Hard Threesome | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Babe Hard Threesome | source=registry	
2025-11-03T10:03:31.049112Z	shellbag	[Session 144] ■ Folder Viewed y Piss!ng on Face 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Piss!ng on Face 1 | source=registry	
2025-11-03T10:03:31.049112Z	shellbag	[Session 144] ■ Folder Viewed vegf-Pt02 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Piss!ng on Face 1\vegf-Pt02 | source=registry	
2025-11-03T10:03:40.576232Z	shellbag	[Session 144] ■ Folder Viewed y Piss!ng on Face | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Piss!ng on Face | source=registry	
2025-11-03T10:03:40.576232Z	shellbag	[Session 144] ■ Folder Viewed vegf-Pt01 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \y Piss!ng on Face\vegf-Pt01 | source=registry	
2025-11-03T10:03:54.547222Z	shellbag	[Session 144] ■ Folder Viewed ousin pics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ousin pics | source=registry	
2025-11-03T10:03:54.547222Z	shellbag	[Session 144] ■ Folder Viewed ousin pics | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ousin pics\ousin pics | source=registry	
2025-11-03T10:04:06.467822Z	shellbag	[Session 144] ■ Folder Viewed ning Hindi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ning Hindi | source=registry	
2025-11-03T10:04:06.467822Z	shellbag	[Session 144] ■ Folder Viewed Old | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ning Hindi\Old | source=registry	
2025-11-03T10:04:19.077782Z	shellbag	[Session 144] ■ Folder Viewed GF SHOWING HAIRY BUSHY | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ GF SHOWING HAIRY BUSHY | source=registry	
2025-11-03T10:04:19.077782Z	shellbag	[Session 144] ■ Folder Viewed SMISH_showing_hairy_bush | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ GF SHOWING HAIRY BUSHY\SMISH_showing_hairy_bush | source=registry	
2025-11-03T10:04:29.415552Z	shellbag	[Session 144] ■ Folder Viewed terial Indian Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \terial Indian Girl | source=registry	
2025-11-03T10:04:29.416540Z	shellbag	[Session 144] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \terial Indian Girl\■ | source=registry	

Session 145 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-03T10:11:05.114692Z	shellbag	[Session 145] ■ Folder Viewed Outdoor Sucking | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Outdoor Sucking | source=registry	
2025-11-03T10:11:11.163172Z	shellbag	[Session 145] ■ Folder Viewed ewly Married | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ewly Married | source=registry	

Session 146 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-05T04:59:59.719526Z	shellbag	[Session 146] ■ Folder Viewed utube Eruma Saani Shyni Blowjob & Full Leaks | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \utube Eruma Saani Shyni Blowjob & Full Leaks | source=registry	

Session 147 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-06T07:02:53.801418Z	shellbag	[Session 147] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \> | source=registry	
2025-11-06T07:02:53.801418Z	shellbag	[Session 147] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \>\> | source=registry	
2025-11-06T07:02:58.263346Z	shellbag	[Session 147] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \ | source=registry	

Session 148 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-06T07:08:34.169740Z	shellbag	[Session 148] ■ Folder Viewed {90E24D373F126545916439C4925E467B} | CLSID\{90E24D373F126545916439C4925E467B} | source=registry	

Session 149 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-07T09:14:58.373532Z	shellbag	[Session 149] ■ Folder Viewed > | CLSID\{2F0010B7A6F519002F453A5C00000000}\@\> | source=registry	
2025-11-07T09:15:05.461324Z	shellbag	[Session 149] ■ Folder Viewed @ | CLSID\{2F0010B7A6F519002F453A5C00000000}\@ | source=registry	

Session 150 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-07T09:26:15.873020Z	prefetch	[Session 150] ■ Executed Program (runs: 3) DFRGUI.EXE-AD62D9FA.pf | C:/Windows/Prefetch\DFRGUI.EXE-AD62D9FA.pf | exe=DFRGUI.EXE | source=local:poor_billionaire, pref_hash=ad62d9fa, files_count=57, volumes_count=1	
2025-11-07T09:26:15.873020Z	prefetch	[Session 150] ■ Executed Program (runs: 3) DFRGUI.EXE-AD62D9FA.pf | C:/Windows/Prefetch\DFRGUI.EXE-AD62D9FA.pf | exe=DFRGUI.EXE | source=local:poor_billionaire, pref_hash=ad62d9fa, files_count=57, volumes_count=1	
2025-11-07T09:26:15.873020Z	prefetch	[Session 150] ■ Executed Program (runs: 3) DFRGUI.EXE-AD62D9FA.pf | C:/Windows/Prefetch\DFRGUI.EXE-AD62D9FA.pf | exe=DFRGUI.EXE | source=local:poor_billionaire, pref_hash=ad62d9fa, files_count=57, volumes_count=1	

Session 151 — 5 event(s)

Time	Type	Detail	Anomaly
2025-11-08T16:37:07.513206Z	shellbag	[Session 151] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ny College Girl\ | source=registry	
2025-11-08T16:37:07.514204Z	shellbag	[Session 151] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ny College Girl\ \> | source=registry	
2025-11-08T16:37:30.344448Z	shellbag	[Session 151] ■ Folder Viewed sky Teen Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \sky Teen Girl | source=registry	
2025-11-08T16:39:08.488798Z	shellbag	[Session 151] ■ Folder Viewed ny College Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ny College Girl | source=registry	
2025-11-08T16:39:08.489714Z	shellbag	[Session 151] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ny College Girl\> | source=registry	

Session 152 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-08T16:51:27.640928Z	shellbag	[Session 152] ■ Folder Viewed w MmsHunt | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \w MmsHunt | source=registry	

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-11-08T16:51:27.640928Z</td><td>shellbag</td><td>[Session 152] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \w MmsHunt\ | source=registry</td><td></td></tr>
</table>

Session 153 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-08T16:53:55.501734Z	shellbag	[Session 153] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Milky Body Kannada Wife\■ | source=registry	

Session 154 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-08T17:50:58.569520Z	shellbag	[Session 154] ■ Folder Viewed {D903D5DFA323CB03040000000000C703} | CLSID\{D903D5DFA323CB03040000000000C703} | source=registry	

Session 155 — 15 event(s)

Time	Type	Detail	Anomaly
2025-11-08T18:36:41.806620Z	shellbag	[Session 155] ■ Folder Viewed fluencer Giving Blowjob Threesome1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Giving Blowjob Threesome1 | source=registry	
2025-11-08T18:37:27.894950Z	shellbag	[Session 155] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Giving Blowjob Threesome\> | source=registry	
2025-11-08T18:37:33.427458Z	shellbag	[Session 155] ■ Folder Viewed os | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Giving Blowjob Threesome\os | source=registry	
2025-11-08T18:37:42.899020Z	shellbag	[Session 155] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Giving Blowjob Threesome\ | source=registry	
2025-11-08T18:38:06.412280Z	shellbag	[Session 155] ■ Folder Viewed fluencer Giving Blowjob Threesome | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \fluencer Giving Blowjob Threesome | source=registry	
2025-11-08T18:38:14.323468Z	shellbag	[Session 155] ■ Folder Viewed reesome Couple Blowjob | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \reesome Couple Blowjob | source=registry	
2025-11-08T18:38:14.323468Z	shellbag	[Session 155] ■ Folder Viewed Sm | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \reesome Couple Blowjob\Sm | source=registry	
2025-11-08T18:38:23.622708Z	shellbag	[Session 155] ■ Folder Viewed ls Threesome Fun | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ls Threesome Fun | source=registry	
2025-11-08T18:38:55.204848Z	shellbag	[Session 155] ■ Folder Viewed ian Housewife Hard Threesome | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ian Housewife Hard Threesome | source=registry	
2025-11-08T18:38:55.204848Z	shellbag	[Session 155] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ian Housewife Hard Threesome\ | source=registry	
2025-11-08T18:39:12.352824Z	shellbag	[Session 155] ■ Folder Viewed lhi Girl Hard Threesome | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lhi Girl Hard Threesome | source=registry	

Time	Type	Detail	Anomaly
2025-11-08T18:39:12.352824Z	shellbag	[Session 155] ■ Folder Viewed Dose__newfilesheng | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \lhi Girl Hard Threesome\Dose__newfilesheng | source=registry	
2025-11-08T18:39:46.379930Z	shellbag	[Session 155] ■ Folder Viewed with Bull in Hotel | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \with Bull in Hotel | source=registry	
2025-11-08T18:39:47.714840Z	shellbag	[Session 155] ■ Folder Viewed ThreSome | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \with Bull in Hotel\ThreSome | source=registry	
2025-11-08T18:39:47.714840Z	shellbag	[Session 155] ■ Folder Viewed l Sxi Bhabi Sucking Dick Licking Pussy Slap Hard Sexy Ass Fucking Hard From Bheind Threesome Dirty Talkig HINDI Audio 12Mint Video | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \with Bull in Hotel\ThreSome\l Sxi Bhabi Sucking Dick Licking Pussy Slap Hard Sexy Ass Fucking Hard From Bheind Threesome Dirty Talkig HINDI Audio 12Mint Video | source=registry	

Session 156 — 18 event(s)

Time	Type	Detail	Anomaly
2025-11-08T18:43:31.880818Z	shellbag	[Session 156] ■ Folder Viewed Part2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\Part2 | source=registry	
2025-11-08T18:43:39.001520Z	shellbag	[Session 156] ■ Folder Viewed Part1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\Part1 | source=registry	
2025-11-08T18:43:39.001520Z	shellbag	[Session 156] ■ Folder Viewed k Part 1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\Part1\k Part 1 | source=registry	
2025-11-08T18:44:19.916350Z	shellbag	[Session 156] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\@ | source=registry	
2025-11-08T18:44:19.916350Z	shellbag	[Session 156] ■ Folder Viewed ucking | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\@\ucking | source=registry	
2025-11-08T18:45:14.130982Z	shellbag	[Session 156] ■ Folder Viewed Part | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\Part | source=registry	
2025-11-08T18:46:12.381578Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ | source=registry	
2025-11-08T18:46:12.381578Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ \ | source=registry	
2025-11-08T18:46:24.114014Z	shellbag	[Session 156] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\> | source=registry	
2025-11-08T18:46:24.114014Z	shellbag	[Session 156] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\>\> | source=registry	

Time	Type	Detail	Anomaly
2025-11-08T18:47:24.883424Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ | source=registry	
2025-11-08T18:47:24.883424Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ \ | source=registry	
2025-11-08T18:47:49.188592Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ | source=registry	
2025-11-08T18:47:49.189592Z	shellbag	[Session 156] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ \■ | source=registry	
2025-11-08T18:48:32.108372Z	shellbag	[Session 156] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\@ | source=registry	
2025-11-08T18:48:32.108372Z	shellbag	[Session 156] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\@\@ | source=registry	
2025-11-08T18:49:09.632688Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ \ | source=registry	
2025-11-08T18:49:21.311226Z	shellbag	[Session 156] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l\ | source=registry	

Session 157 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-10T05:54:04.401262Z	shellbag	[Session 157] ■ Folder Viewed sExplorer | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\sExplorer\sExplorer | source=registry	

Session 158 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-10T06:41:52.635626Z	shellbag	[Session 158] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ | source=registry	

Session 159 — 4 event(s)

Time	Type	Detail	Anomaly
2025-11-10T13:10:17.374870Z	shellbag	[Session 159] ■ Folder Viewed HUNT__Picsvids | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__Picsvids | source=registry	
2025-11-10T13:10:39.313278Z	shellbag	[Session 159] ■ Folder Viewed HUNT__628182872 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__628182872 | source=registry	
2025-11-10T13:10:39.313278Z	shellbag	[Session 159] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__628182872\> | source=registry	
2025-11-10T13:10:59.307098Z	shellbag	[Session 159] ■ Folder Viewed HUNT__NewHotty | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \HUNT__NewHotty | source=registry	

Session 160 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-10T18:46:23.738558Z	shellbag	[Session 160] ■ Folder Viewed shevad | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ shevad | source=registry	
2025-11-10T18:46:23.739554Z	shellbag	[Session 160] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ shevad\> | source=registry	
2025-11-10T18:46:39.680066Z	shellbag	[Session 160] ■ Folder Viewed jabi Girl | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \jabi Girl | source=registry	

Session 161 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-11T12:47:07.492312Z	shellbag	[Session 161] ■ Folder Viewed Cuck Wife Threesome Fucking | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Cuck Wife Threesome Fucking | source=registry	
2025-11-11T12:48:35.612052Z	shellbag	[Session 161] ■ Folder Viewed mallu | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \mallu | source=registry	
2025-11-11T12:49:12.532374Z	shellbag	[Session 161] ■ Folder Viewed king in Kitchen | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \king in Kitchen | source=registry	

Session 162 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-13T08:19:03.669359Z	prefetch	[Session 162] ■ Executed Program (runs: 3) CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | C:/Windows/Prefetch\CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | exe=CREDENTIALUIBROKER.EXE | source=local:poor_billionaire, pref_hash=8ceda3eb, files_count=243, volumes_count=1	
2025-11-13T08:19:03.669359Z	prefetch	[Session 162] ■ Executed Program (runs: 3) CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | C:/Windows/Prefetch\CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | exe=CREDENTIALUIBROKER.EXE | source=local:poor_billionaire, pref_hash=8ceda3eb, files_count=243, volumes_count=1	
2025-11-13T08:19:03.669359Z	prefetch	[Session 162] ■ Executed Program (runs: 3) CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | C:/Windows/Prefetch\CREDENTIALUIBROKER.EXE-8CEDA3EB.pf | exe=CREDENTIALUIBROKER.EXE | source=local:poor_billionaire, pref_hash=8ceda3eb, files_count=243, volumes_count=1	

Session 163 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-14T06:32:54.510524Z	shellbag	[Session 163] ■ Folder Viewed {2F0010B7A6F519002F453A5C00000000} | CLSID\{2F0010B7A6F519002F453A5C00000000} | source=registry	
2025-11-14T06:34:15.906326Z	shellbag	[Session 163] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \ | source=registry	

Session 164 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-14T06:52:35.402552Z	shellbag	[Session 164] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Session 165 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-14T07:20:31.343298Z	shellbag	[Session 165] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	

Session 166 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-14T08:00:55.262038Z	shellbag	[Session 166] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	

Session 167 — 5 event(s)

Time	Type	Detail	Anomaly
2025-11-14T08:11:30.858354Z	shellbag	[Session 167] ■ Folder Viewed les | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\les | source=registry	
2025-11-14T08:11:33.449320Z	shellbag	[Session 167] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\s | source=registry	
2025-11-14T08:11:35.555016Z	shellbag	[Session 167] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\s | source=registry	
2025-11-14T08:11:37.635234Z	shellbag	[Session 167] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\s | source=registry	
2025-11-14T08:11:39.821632Z	shellbag	[Session 167] ■ Folder Viewed es | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\es | source=registry	

Session 168 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-14T08:33:07.063266Z	shellbag	[Session 168] ■ Folder Viewed > | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\> | source=registry	

Session 169 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-14T09:51:47.350239Z	prefetch	[Session 169] ■ Executed Program (runs: 7) CHXSMARTSCREEN.EXE-B95BCB2E.pf | C:/Windows/Prefetch\CHXSMARTSCREEN.EXE-B95BCB2E.pf | exe=CHXSMARTSCREEN.EXE | source=local:poor_billionaire, pref_hash=b95bcb2e, files_count=129, volumes_count=1	
2025-11-14T09:51:47.350239Z	prefetch	[Session 169] ■ Executed Program (runs: 7) CHXSMARTSCREEN.EXE-B95BCB2E.pf | C:/Windows/Prefetch\CHXSMARTSCREEN.EXE-B95BCB2E.pf | exe=CHXSMARTSCREEN.EXE | source=local:poor_billionaire, pref_hash=b95bcb2e, files_count=129, volumes_count=1	
2025-11-14T09:51:47.350239Z	prefetch	[Session 169] ■ Executed Program (runs: 7) CHXSMARTSCREEN.EXE-B95BCB2E.pf | C:/Windows/Prefetch\CHXSMARTSCREEN.EXE-B95BCB2E.pf | exe=CHXSMARTSCREEN.EXE | source=local:poor_billionaire, pref_hash=b95bcb2e, files_count=129, volumes_count=1	

Session 170 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-14T10:36:39.301934Z	shellbag	[Session 170] ■ Folder Viewed g | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\g | source=registry	

Session 171 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-17T05:41:28.732138Z	shellbag	[Session 171] ■ Folder Viewed itable-linux-2.0.0.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\itable-linux-2.0.0.zip | source=registry	
2025-11-17T05:42:07.568654Z	shellbag	[Session 171] ■ Folder Viewed itable-linux-2.0.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\itable-linux-2.0.0 | source=registry	
2025-11-17T05:42:07.569668Z	shellbag	[Session 171] ■ Folder Viewed itable2-Linux | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\\itable-linux-2.0.0\itable2-Linux | source=registry	

Session 172 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-17T05:46:26.431738Z	shellbag	[Session 172] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Session 173 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-17T07:12:03.190438Z	shellbag	[Session 173] ■ Folder Viewed {471A0359723FA74489C55595FE6B30EE} | CLSID\{471A0359723FA74489C55595FE6B30EE} | source=registry	

Session 174 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-19T11:35:24.993288Z	shellbag	[Session 174] ■ Folder Viewed l Milky Body Kannada Wife | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Milky Body Kannada Wife | source=registry	
2025-11-19T11:35:24.993288Z	shellbag	[Session 174] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l Milky Body Kannada Wife\■ | source=registry	

Session 175 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-20T18:11:11.253434Z	shellbag	[Session 175] ■ Folder Viewed a | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\a | source=registry	

Session 176 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-20T21:02:00.266789Z	prefetch	[Session 176] ■ Executed Program (runs: 7) DLLHOST.EXE-F6E270D2.pf | C:/Windows/Prefetch\DLLHOST.EXE-F6E270D2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=f6e270d2, files_count=43, volumes_count=1	
2025-11-20T21:02:00.266789Z	prefetch	[Session 176] ■ Executed Program (runs: 7) DLLHOST.EXE-F6E270D2.pf | C:/Windows/Prefetch\DLLHOST.EXE-F6E270D2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=f6e270d2, files_count=43, volumes_count=1	
2025-11-20T21:02:00.266789Z	prefetch	[Session 176] ■ Executed Program (runs: 7) DLLHOST.EXE-F6E270D2.pf | C:/Windows/Prefetch\DLLHOST.EXE-F6E270D2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=f6e270d2, files_count=43, volumes_count=1	

Session 177 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-20T21:39:22.646124Z	shellbag	[Session 177] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\■ | source=registry	

Session 178 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-21T07:13:10.423844Z	shellbag	[Session 178] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\l | source=registry	
2025-11-21T07:13:10.423844Z	shellbag	[Session 178] ■ Folder Viewed ssed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\l\ssed | source=registry	

Session 179 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-21T08:37:12.182326Z	shellbag	[Session 179] ■ Folder Viewed u | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\u | source=registry	
2025-11-21T08:37:12.182326Z	shellbag	[Session 179] ■ Folder Viewed ssed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\u\ssed | source=registry	

Session 180 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-23T12:02:51.319150Z	shellbag	[Session 180] ■ Folder Viewed l | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \l | source=registry	

Session 181 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-23T16:06:42.405632Z	shellbag	[Session 181] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\@\t\ | source=registry	

Session 182 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-25T22:27:51.314470Z	shellbag	[Session 182] ■ Folder Viewed l Transactions Dataset | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\l Transactions Dataset | source=registry	

Session 183 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-25T22:43:06.927280Z	shellbag	[Session 183] ■ Folder Viewed l Transactions Dataset | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\l Transactions Dataset\l Transactions Dataset | source=registry	

Session 184 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-25T23:00:34.751816Z	shellbag	[Session 184] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	

Session 185 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-26T08:23:58.465632Z	shellbag	[Session 185] ■ Folder Viewed E:\ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\E:\ | source=registry	

Session 186 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-26T16:41:53.243976Z	shellbag	[Session 186] ■ Folder Viewed Dose__ANUJSINGHCOLLECTIONSPICSVIDS3066 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \Dose__ANUJSINGHCOLLECTIONSPICSVIDS3066 | source=registry	
2025-11-26T16:42:00.968982Z	shellbag	[Session 186] ■ Folder Viewed ried_ybhabhi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ried_ybhabhi | source=registry	
2025-11-26T16:42:00.968982Z	shellbag	[Session 186] ■ Folder Viewed rried_horny_bhabhi | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ried_ybhabhi\rried_horny_bhabhi | source=registry	

Session 187 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-26T18:33:12.855784Z	shellbag	[Session 187] ■ Folder Viewed ject | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ject | source=registry	
2025-11-26T18:33:12.855784Z	shellbag	[Session 187] ■ Folder Viewed s | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ject\s | source=registry	

Session 188 — 1 event(s)

Time	Type	Detail	Anomaly
2025-11-27T12:17:32.952032Z	shellbag	[Session 188] ■ Folder Viewed ll | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ \ll | source=registry	

Session 189 — 2 event(s)

Time	Type	Detail	Anomaly
2025-11-29T17:30:37.136894Z	shellbag	[Session 189] ■ Folder Viewed zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\zip | source=registry	
2025-11-29T17:30:49.285212Z	shellbag	[Session 189] ■ Folder Viewed ject.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ject.zip | source=registry	

Session 190 — 3 event(s)

Time	Type	Detail	Anomaly
2025-11-29T17:32:51.384456Z	shellbag	[Session 190] ■ Folder Viewed nment | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment | source=registry	
2025-11-29T17:32:52.494784Z	shellbag	[Session 190] ■ Folder Viewed d | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\nment\d | source=registry	
2025-11-29T17:34:36.544640Z	shellbag	[Session 190] ■ Folder Viewed gs_Parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\gs_Parser | source=registry	

Session 191 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-01T20:32:47.002380Z	shellbag	[Session 191] ■ Folder Viewed er | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er | source=registry	

Session 192 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-03T08:20:13.556672Z	shellbag	[Session 192] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser | source=registry	

Session 193 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-03T08:30:33.231010Z	shellbag	[Session 193] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\@ | source=registry	

Session 194 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-03T08:44:35.861976Z	shellbag	[Session 194] ■ Folder Viewed .Bin | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\.Bin | source=registry	

Session 195 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T11:11:44.445714Z	shellbag	[Session 195] ■ Folder Viewed {D903D5DFA323CB03040000000000C703} | CLSID\{D903D5DFA323CB03040000000000C703} | source=registry	

Session 196 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T11:16:32.259188Z	shellbag	[Session 196] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ \>\ \er\ | source=registry	

Session 197 — 4 event(s)

Time	Type	Detail	Anomaly
2025-12-06T17:48:04.907976Z	shellbag	[Session 197] ■ Folder Viewed e__ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\e__ | source=registry	
2025-12-06T17:50:03.247174Z	shellbag	[Session 197] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\ | source=registry	
2025-12-06T17:50:05.666430Z	shellbag	[Session 197] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\ \■ | source=registry	
2025-12-06T17:50:05.667884Z	shellbag	[Session 197] ■ Folder Viewed kages | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\ \■\kages | source=registry	

Session 198 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T18:13:08.029340Z	shellbag	[Session 198] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser\■ | source=registry	

Session 199 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T18:55:26.689016Z	shellbag	[Session 199] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\@ | source=registry	

Session 200 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T19:06:03.171898Z	shellbag	[Session 200] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser\artifacts-parser | source=registry	

Session 201 — 4 event(s)

Time	Type	Detail	Anomaly
2025-12-06T21:20:51.741796Z	shellbag	[Session 201] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\■ | source=registry	
2025-12-06T21:21:26.006870Z	shellbag	[Session 201] ■ Folder Viewed artifacts-parser.zip | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser.zip | source=registry	
2025-12-06T21:21:42.649580Z	shellbag	[Session 201] ■ Folder Viewed artifacts-parser-v1.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.0 | source=registry	
2025-12-06T21:21:42.649580Z	shellbag	[Session 201] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.0\artifacts-parser | source=registry	

Session 202 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T21:26:30.071836Z	shellbag	[Session 202] ■ Folder Viewed artifacts-parser-v2.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0 | source=registry	

Session 203 — 4 event(s)

Time	Type	Detail	Anomaly
2025-12-06T21:28:50.680166Z	shellbag	[Session 203] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser\ | source=registry	
2025-12-06T21:28:50.680166Z	shellbag	[Session 203] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser\ \@ | source=registry	
2025-12-06T21:28:56.970062Z	shellbag	[Session 203] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser\@ | source=registry	
2025-12-06T21:28:59.701004Z	shellbag	[Session 203] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser\■ | source=registry	

Session 204 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T21:53:15.373612Z	shellbag	[Session 204] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser\■ | source=registry	

Session 205 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T21:56:42.245108Z	lnk	[Session 205] ■ Shortcut / LNK Visual Studio Code.lnk | C:/Users/mukul/AppData/Roaming/Microsoft/Windows\Start Menu\Programs\Visual Studio Code\Visual Studio Code.lnk | target=C:\Users\mukul\AppData\Local\Programs\Microsoft VS Code\Code.exe | source=pylnk3	

Session 206 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-06T22:58:12.645536Z	shellbag	[Session 206] ■ Folder Viewed artifacts-parser-v1.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1 | source=registry	

Session 207 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-07T21:09:56.284408Z	shellbag	[Session 207] ■ Folder Viewed artifacts-parser-v1.2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2 | source=registry	

Session 208 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-07T21:14:27.790326Z	shellbag	[Session 208] ■ Folder Viewed artifacts-parser-v1.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser-v1.1 | source=registry	
2025-12-07T21:14:27.791322Z	shellbag	[Session 208] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser-v1.1\artifacts-parser | source=registry	

Session 209 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-07T21:19:33.288552Z	shellbag	[Session 209] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1\artifacts-parser | source=registry	
2025-12-07T21:19:33.288552Z	shellbag	[Session 209] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1\artifacts-parser\@ | source=registry	

Session 210 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-07T21:44:15.191589Z	prefetch	[Session 210] ■ Executed Program (runs: 0) BASENAME.EXE-E7DC3D6A.pf | C:/Windows/Prefetch\BASENAME.EXE-E7DC3D6A.pf | exe=BASENAME.EXE | source=local:poor_billionaire, pref_hash=e7dc3d6a, files_count=17, volumes_count=1	
2025-12-07T21:44:15.191589Z	prefetch	[Session 210] ■ Executed Program (runs: 0) BASENAME.EXE-E7DC3D6A.pf | C:/Windows/Prefetch\BASENAME.EXE-E7DC3D6A.pf | exe=BASENAME.EXE | source=local:poor_billionaire, pref_hash=e7dc3d6a, files_count=17, volumes_count=1	
2025-12-07T21:44:15.191589Z	prefetch	[Session 210] ■ Executed Program (runs: 0) BASENAME.EXE-E7DC3D6A.pf | C:/Windows/Prefetch\BASENAME.EXE-E7DC3D6A.pf | exe=BASENAME.EXE | source=local:poor_billionaire, pref_hash=e7dc3d6a, files_count=17, volumes_count=1	

Session 211 — 6 event(s)

Time	Type	Detail	Anomaly
2025-12-07T21:50:55.243917Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CSC.EXE-B6D5E435.pf | C:/Windows/Prefetch\CSC.EXE-B6D5E435.pf | exe=CSC.EXE | source=local:poor_billionaire, pref_hash=b6d5e435, files_count=66, volumes_count=1	
2025-12-07T21:50:55.243917Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CSC.EXE-B6D5E435.pf | C:/Windows/Prefetch\CSC.EXE-B6D5E435.pf | exe=CSC.EXE | source=local:poor_billionaire, pref_hash=b6d5e435, files_count=66, volumes_count=1	
2025-12-07T21:50:55.243917Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CSC.EXE-B6D5E435.pf | C:/Windows/Prefetch\CSC.EXE-B6D5E435.pf | exe=CSC.EXE | source=local:poor_billionaire, pref_hash=b6d5e435, files_count=66, volumes_count=1	
2025-12-07T21:50:55.318489Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CVTRES.EXE-BBD3ED93.pf | C:/Windows/Prefetch\CVTRES.EXE-BBD3ED93.pf | exe=CVTRES.EXE | source=local:poor_billionaire, pref_hash=bbd3ed93, files_count=31, volumes_count=1	
2025-12-07T21:50:55.318489Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CVTRES.EXE-BBD3ED93.pf | C:/Windows/Prefetch\CVTRES.EXE-BBD3ED93.pf | exe=CVTRES.EXE | source=local:poor_billionaire, pref_hash=bbd3ed93, files_count=31, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-07T21:50:55.318489Z	prefetch	[Session 211] ■ Executed Program (runs: 0) CVTRES.EXE-BBD3ED93.pf | C:/Windows/Prefetch\CVTRES.EXE-BBD3ED93.pf | exe=CVTRES.EXE | source=local:poor_billionaire, pref_hash=bbd3ed93, files_count=31, volumes_count=1	

Session 212 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-07T22:32:31.379252Z	shellbag	[Session 212] ■ Folder Viewed artifacts-parser-v1.1.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.1 | source=registry	

Session 213 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-07T22:37:14.527568Z	shellbag	[Session 213] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.1\artifacts-parser\@ | source=registry	

Session 214 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-08T05:16:11.461426Z	shellbag	[Session 214] ■ Folder Viewed artifacts-parser-v1.1.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser-v1.1.1 | source=registry	
2025-12-08T05:16:11.461426Z	shellbag	[Session 214] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\artifacts-parser-v1.1.1\artifacts-parser | source=registry	

Session 215 — 6 event(s)

Time	Type	Detail	Anomaly
2025-12-08T05:25:40.652279Z	prefetch	[Session 215] ■ Executed Program (runs: 0) DEVICES.EXE-C2EFC6C7.pf | C:/Windows/Prefetch\DEVICES.EXE-C2EFC6C7.pf | exe=DEVICES.EXE | source=local:poor_billionaire, pref_hash=c2efc6c7, files_count=99, volumes_count=1	
2025-12-08T05:25:40.652279Z	prefetch	[Session 215] ■ Executed Program (runs: 0) DEVICES.EXE-C2EFC6C7.pf | C:/Windows/Prefetch\DEVICES.EXE-C2EFC6C7.pf | exe=DEVICES.EXE | source=local:poor_billionaire, pref_hash=c2efc6c7, files_count=99, volumes_count=1	
2025-12-08T05:25:40.652279Z	prefetch	[Session 215] ■ Executed Program (runs: 0) DEVICES.EXE-C2EFC6C7.pf | C:/Windows/Prefetch\DEVICES.EXE-C2EFC6C7.pf | exe=DEVICES.EXE | source=local:poor_billionaire, pref_hash=c2efc6c7, files_count=99, volumes_count=1	
2025-12-08T05:26:07.401592Z	prefetch	[Session 215] ■ Executed Program (runs: 0) CHK.EXE-7F0B90B8.pf | C:/Windows/Prefetch\CHK.EXE-7F0B90B8.pf | exe=CHK.EXE | source=local:poor_billionaire, pref_hash=7f0b90b8, files_count=31, volumes_count=1	
2025-12-08T05:26:07.401592Z	prefetch	[Session 215] ■ Executed Program (runs: 0) CHK.EXE-7F0B90B8.pf | C:/Windows/Prefetch\CHK.EXE-7F0B90B8.pf | exe=CHK.EXE | source=local:poor_billionaire, pref_hash=7f0b90b8, files_count=31, volumes_count=1	
2025-12-08T05:26:07.401592Z	prefetch	[Session 215] ■ Executed Program (runs: 0) CHK.EXE-7F0B90B8.pf | C:/Windows/Prefetch\CHK.EXE-7F0B90B8.pf | exe=CHK.EXE | source=local:poor_billionaire, pref_hash=7f0b90b8, files_count=31, volumes_count=1	

Session 216 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-08T05:41:30.743056Z	shellbag	[Session 216] ■ Folder Viewed artifacts-parser-v2.0 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v2.0 | source=registry	
2025-12-08T05:41:30.743056Z	shellbag	[Session 216] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v2.0\artifacts-parser | source=registry	

Session 217 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-08T07:06:33.167148Z	shellbag	[Session 217] ■ Folder Viewed {0504D5DFA323F703040000000000F303} | CLSID\{0504D5DFA323F703040000000000F303} | source=registry	

Session 218 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-08T07:21:41.649832Z	shellbag	[Session 218] ■ Folder Viewed {0504D5DFA323F703040000000000F303} | CLSID\{0504D5DFA323F703040000000000F303} | source=registry	

Session 219 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-08T07:28:38.279487Z	prefetch	[Session 219] ■ Executed Program (runs: 0) DLLHOST.EXE-ECDCED3C.pf | C:/Windows/Prefetch\DLLHOST.EXE-ECDCED3C.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=ecdced3c, files_count=30, volumes_count=1	
2025-12-08T07:28:38.279487Z	prefetch	[Session 219] ■ Executed Program (runs: 0) DLLHOST.EXE-ECDCED3C.pf | C:/Windows/Prefetch\DLLHOST.EXE-ECDCED3C.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=ecdced3c, files_count=30, volumes_count=1	
2025-12-08T07:28:38.279487Z	prefetch	[Session 219] ■ Executed Program (runs: 0) DLLHOST.EXE-ECDCED3C.pf | C:/Windows/Prefetch\DLLHOST.EXE-ECDCED3C.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=ecdced3c, files_count=30, volumes_count=1	

Session 220 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-08T20:57:27.444067Z	prefetch	[Session 220] ■ Executed Program (runs: 0) DLLHOST.EXE-D52C49C5.pf | C:/Windows/Prefetch\DLLHOST.EXE-D52C49C5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=d52c49c5, files_count=53, volumes_count=1	
2025-12-08T20:57:27.444067Z	prefetch	[Session 220] ■ Executed Program (runs: 0) DLLHOST.EXE-D52C49C5.pf | C:/Windows/Prefetch\DLLHOST.EXE-D52C49C5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=d52c49c5, files_count=53, volumes_count=1	
2025-12-08T20:57:27.444067Z	prefetch	[Session 220] ■ Executed Program (runs: 0) DLLHOST.EXE-D52C49C5.pf | C:/Windows/Prefetch\DLLHOST.EXE-D52C49C5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=d52c49c5, files_count=53, volumes_count=1	

Session 221 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-08T21:56:30.279589Z	prefetch	[Session 221] ■ Executed Program (runs: 0) AI.EXE-C5B0F666.pf | C:/Windows/Prefetch\AI.EXE-C5B0F666.pf | exe=AI.EXE | source=local:poor_billionaire, pref_hash=c5b0f666, files_count=57, volumes_count=1	
2025-12-08T21:56:30.279589Z	prefetch	[Session 221] ■ Executed Program (runs: 0) AI.EXE-C5B0F666.pf | C:/Windows/Prefetch\AI.EXE-C5B0F666.pf | exe=AI.EXE | source=local:poor_billionaire, pref_hash=c5b0f666, files_count=57, volumes_count=1	
2025-12-08T21:56:30.279589Z	prefetch	[Session 221] ■ Executed Program (runs: 0) AI.EXE-C5B0F666.pf | C:/Windows/Prefetch\AI.EXE-C5B0F666.pf | exe=AI.EXE | source=local:poor_billionaire, pref_hash=c5b0f666, files_count=57, volumes_count=1	

Session 222 — 4 event(s)

Time	Type	Detail	Anomaly
2025-12-08T22:18:08.454062Z	shellbag	[Session 222] ■ Folder Viewed artifacts-parser-v1.1.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v1.1.1 | source=registry	
2025-12-08T22:18:11.212996Z	shellbag	[Session 222] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v1.1.1\artifacts-parser | source=registry	
2025-12-08T22:18:11.212996Z	shellbag	[Session 222] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v1.1.1\artifacts-parser\@ | source=registry	
2025-12-08T22:18:27.075612Z	shellbag	[Session 222] ■ Folder Viewed [M[M. | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.1\artifacts-parser\[M[M. | source=registry	

Session 223 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-08T22:46:01.053728Z	shellbag	[Session 223] ■ Folder Viewed e | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.1\artifacts-parser\e | source=registry	

Session 224 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-08T22:59:03.524192Z	shellbag	[Session 224] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.1\artifacts-parser | source=registry	

Session 225 — 3 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-12-08T23:07:36.678636Z</td><td>prefetch</td><td>[Session 225] ■ Executed Program (runs: 0) CHCP.COM-2CF9B15C.pf | C:/Windows/Prefetch\CHCP.COM-2CF9B15C.pf | exe=CHCP.COM | source=local:poor_billionaire, pref_hash=2cf9b15c, files_count=12, volumes_count=1</td><td></td></tr>
<tr><td>2025-12-08T23:07:36.678636Z</td><td>prefetch</td><td>[Session 225] ■ Executed Program (runs: 0) CHCP.COM-2CF9B15C.pf | C:/Windows/Prefetch\CHCP.COM-2CF9B15C.pf | exe=CHCP.COM | source=local:poor_billionaire, pref_hash=2cf9b15c, files_count=12, volumes_count=1</td><td></td></tr>
<tr><td>2025-12-08T23:07:36.678636Z</td><td>prefetch</td><td>[Session 225] ■ Executed Program (runs: 0) CHCP.COM-2CF9B15C.pf | C:/Windows/Prefetch\CHCP.COM-2CF9B15C.pf | exe=CHCP.COM | source=local:poor_billionaire, pref_hash=2cf9b15c, files_count=12, volumes_count=1</td><td></td></tr>
</table>

Session 226 — 2 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-12-08T23:23:21.307004Z</td><td>shellbag</td><td>[Session 226] ■ Folder Viewed artifacts-parser-v1.1.2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.2 | source=registry</td><td></td></tr>
<tr><td>2025-12-08T23:23:22.987682Z</td><td>shellbag</td><td>[Session 226] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.2\artifacts-parser\@ | source=registry</td><td></td></tr>
</table>

Session 227 — 6 event(s)

<table>
<tr><th>Time</th><th>Type</th><th>Detail</th><th>Anomaly</th></tr>
<tr><td>2025-12-08T23:41:28.339852Z</td><td>prefetch</td><td>[Session 227] ■ Executed Program (runs: 0) DLLHOST.EXE-895D23F2.pf | C:/Windows/Prefetch\DLLHOST.EXE-895D23F2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=895d23f2, files_count=75, volumes_count=2</td><td></td></tr>
<tr><td>2025-12-08T23:41:28.339852Z</td><td>prefetch</td><td>[Session 227] ■ Executed Program (runs: 0) DLLHOST.EXE-895D23F2.pf | C:/Windows/Prefetch\DLLHOST.EXE-895D23F2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=895d23f2, files_count=75, volumes_count=2</td><td></td></tr>
<tr><td>2025-12-08T23:41:28.339852Z</td><td>prefetch</td><td>[Session 227] ■ Executed Program (runs: 0) DLLHOST.EXE-895D23F2.pf | C:/Windows/Prefetch\DLLHOST.EXE-895D23F2.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=895d23f2, files_count=75, volumes_count=2</td><td></td></tr>
<tr><td>2025-12-08T23:41:40.105840Z</td><td>shellbag</td><td>[Session 227] ■ Folder Viewed artifacts-parser-v1.1.2 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\\artifacts-parser-v1.1.2 | source=registry</td><td></td></tr>
<tr><td>2025-12-08T23:42:05.877504Z</td><td>shellbag</td><td>[Session 227] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2\artifacts-parser | source=registry</td><td></td></tr>
</table>

Time	Type	Detail	Anomaly
2025-12-08T23:42:05.877504Z	shellbag	[Session 227] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2\artifacts-parser\@ | source=registry	

Session 228 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-08T23:44:07.328122Z	shellbag	[Session 228] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v2.0\artifacts-parser | source=registry	

Session 229 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:02:08.003182Z	shellbag	[Session 229] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.2\artifacts-parser\■ | source=registry	

Session 230 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:16:50.417496Z	shellbag	[Session 230] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.2\artifacts-parser | source=registry	

Session 231 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:20:14.985478Z	shellbag	[Session 231] ■ Folder Viewed artifacts-parser-v1.1.3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.3 | source=registry	

Session 232 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:22:28.877902Z	shellbag	[Session 232] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.3\artifacts-parser\■ | source=registry	
2025-12-09T00:22:28.878830Z	shellbag	[Session 232] ■ Folder Viewed e__ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.3\artifacts-parser\■\e__ | source=registry	

Session 233 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:27:25.063418Z	shellbag	[Session 233] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.3\artifacts-parser\@ | source=registry	

Session 234 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T00:56:54.947511Z	prefetch	[Session 234] ■ Executed Program (runs: 0) AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | C:/Windows/Prefetch\AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | exe=AM_DELTA_PATCH_1.441.814.0.EX | source=local:poor_billionaire, pref_hash=5ac300e3, files_count=17, volumes_count=1	
2025-12-09T00:56:54.947511Z	prefetch	[Session 234] ■ Executed Program (runs: 0) AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | C:/Windows/Prefetch\AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | exe=AM_DELTA_PATCH_1.441.814.0.EX | source=local:poor_billionaire, pref_hash=5ac300e3, files_count=17, volumes_count=1	
2025-12-09T00:56:54.947511Z	prefetch	[Session 234] ■ Executed Program (runs: 0) AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | C:/Windows/Prefetch\AM_DELTA_PATCH_1.441.814.0.EX-5AC300E3.pf | exe=AM_DELTA_PATCH_1.441.814.0.EX | source=local:poor_billionaire, pref_hash=5ac300e3, files_count=17, volumes_count=1	

Session 235 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T01:01:56.330979Z	prefetch	[Session 235] ■ Executed Program (runs: 4) DLLHOST.EXE-1803032B.pf | C:/Windows/Prefetch\DLLHOST.EXE-1803032B.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=1803032b, files_count=40, volumes_count=1	
2025-12-09T01:01:56.330979Z	prefetch	[Session 235] ■ Executed Program (runs: 4) DLLHOST.EXE-1803032B.pf | C:/Windows/Prefetch\DLLHOST.EXE-1803032B.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=1803032b, files_count=40, volumes_count=1	
2025-12-09T01:01:56.330979Z	prefetch	[Session 235] ■ Executed Program (runs: 4) DLLHOST.EXE-1803032B.pf | C:/Windows/Prefetch\DLLHOST.EXE-1803032B.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=1803032b, files_count=40, volumes_count=1	

Session 236 — 5 event(s)

Time	Type	Detail	Anomaly
2025-12-09T01:23:59.075586Z	prefetch	[Session 236] ■ Executed Program (runs: 0) DATAEXCHANGEHOST.EXE-8B66795C.pf | C:/Windows/Prefetch\DATAEXCHANGEHOST.EXE-8B66795C.pf | exe=DATAEXCHANGEHOST.EXE | source=local:poor_billionaire, pref_hash=8b66795c, files_count=75, volumes_count=1	
2025-12-09T01:23:59.075586Z	prefetch	[Session 236] ■ Executed Program (runs: 0) DATAEXCHANGEHOST.EXE-8B66795C.pf | C:/Windows/Prefetch\DATAEXCHANGEHOST.EXE-8B66795C.pf | exe=DATAEXCHANGEHOST.EXE | source=local:poor_billionaire, pref_hash=8b66795c, files_count=75, volumes_count=1	
2025-12-09T01:23:59.075586Z	prefetch	[Session 236] ■ Executed Program (runs: 0) DATAEXCHANGEHOST.EXE-8B66795C.pf | C:/Windows/Prefetch\DATAEXCHANGEHOST.EXE-8B66795C.pf | exe=DATAEXCHANGEHOST.EXE | source=local:poor_billionaire, pref_hash=8b66795c, files_count=75, volumes_count=1	
2025-12-09T01:25:06.929000Z	recycle_i	[Session 236] ■ Recycle Bin (deleted file) $IJOIGMA.bat \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IJOIGMA.bat	
2025-12-09T01:25:06.929000Z	recycle_i	[Session 236] ■ Recycle Bin (deleted file) $IJOIGMA.bat \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IJOIGMA.bat	

Session 237 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T01:37:29.105494Z	shellbag	[Session 237] ■ Folder Viewed {D43AAD2469A5304598E1AB02F9417AA8} | CLSID\{D43AAD2469A5304598E1AB02F9417AA8} | source=registry	

Session 238 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-09T01:58:03.171970Z	shellbag	[Session 238] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ | source=registry	
2025-12-09T01:58:04.403418Z	shellbag	[Session 238] ■ Folder Viewed artifacts-parser-v1.1.3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ \artifacts-parser-v1.1.3 | source=registry	

Session 239 — 5 event(s)

Time	Type	Detail	Anomaly
2025-12-09T10:43:05.390878Z	shellbag	[Session 239] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@ | source=registry	
2025-12-09T10:43:05.400664Z	shellbag	[Session 239] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\@ | source=registry	
2025-12-09T10:43:18.158956Z	shellbag	[Session 239] ■ Folder Viewed t | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\@\t | source=registry	
2025-12-09T10:43:18.169036Z	shellbag	[Session 239] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ \@\@\t\@ | source=registry	
2025-12-09T10:45:10.460784Z	shellbag	[Session 239] ■ Folder Viewed | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ \ | source=registry	

Session 240 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-09T11:53:08.085106Z	shellbag	[Session 240] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ \artifacts-parser-v1.1.3\artifacts-parser | source=registry	
2025-12-09T11:53:08.085106Z	shellbag	[Session 240] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\ \artifacts-parser-v1.1.3\artifacts-parser\■ | source=registry	

Session 241 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T12:01:28.545842Z	prefetch	[Session 241] ■ Executed Program (runs: 0) DLLHOST.EXE-6F625E57.pf | C:/Windows/Prefetch\DLLHOST.EXE-6F625E57.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=6f625e57, files_count=26, volumes_count=1	
2025-12-09T12:01:28.545842Z	prefetch	[Session 241] ■ Executed Program (runs: 0) DLLHOST.EXE-6F625E57.pf | C:/Windows/Prefetch\DLLHOST.EXE-6F625E57.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=6f625e57, files_count=26, volumes_count=1	
2025-12-09T12:01:28.545842Z	prefetch	[Session 241] ■ Executed Program (runs: 0) DLLHOST.EXE-6F625E57.pf | C:/Windows/Prefetch\DLLHOST.EXE-6F625E57.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=6f625e57, files_count=26, volumes_count=1	

Session 242 — 6 event(s)

Time	Type	Detail	Anomaly
2025-12-09T13:05:19.467613Z	prefetch	[Session 242] ■ Executed Program (runs: 0) CSRSS.EXE-F3C368CB.pf | C:/Windows/Prefetch\CSRSS.EXE-F3C368CB.pf | exe=CSRSS.EXE | source=local:poor_billionaire, pref_hash=f3c368cb, files_count=39, volumes_count=1	
2025-12-09T13:05:19.467613Z	prefetch	[Session 242] ■ Executed Program (runs: 0) CSRSS.EXE-F3C368CB.pf | C:/Windows/Prefetch\CSRSS.EXE-F3C368CB.pf | exe=CSRSS.EXE | source=local:poor_billionaire, pref_hash=f3c368cb, files_count=39, volumes_count=1	
2025-12-09T13:05:19.467613Z	prefetch	[Session 242] ■ Executed Program (runs: 0) CSRSS.EXE-F3C368CB.pf | C:/Windows/Prefetch\CSRSS.EXE-F3C368CB.pf | exe=CSRSS.EXE | source=local:poor_billionaire, pref_hash=f3c368cb, files_count=39, volumes_count=1	
2025-12-09T13:05:19.590136Z	prefetch	[Session 242] ■ Executed Program (runs: 0) DWM.EXE-314E93C5.pf | C:/Windows/Prefetch\DWM.EXE-314E93C5.pf | exe=DWM.EXE | source=local:poor_billionaire, pref_hash=314e93c5, files_count=113, volumes_count=1	
2025-12-09T13:05:19.590136Z	prefetch	[Session 242] ■ Executed Program (runs: 0) DWM.EXE-314E93C5.pf | C:/Windows/Prefetch\DWM.EXE-314E93C5.pf | exe=DWM.EXE | source=local:poor_billionaire, pref_hash=314e93c5, files_count=113, volumes_count=1	
2025-12-09T13:05:19.590136Z	prefetch	[Session 242] ■ Executed Program (runs: 0) DWM.EXE-314E93C5.pf | C:/Windows/Prefetch\DWM.EXE-314E93C5.pf | exe=DWM.EXE | source=local:poor_billionaire, pref_hash=314e93c5, files_count=113, volumes_count=1	

Session 243 — 15 event(s)

Time	Type	Detail	Anomaly
2025-12-09T14:19:31.734142Z	prefetch	[Session 243] ■ Executed Program (runs: 0) AUTOMODEDETECT.EXE-0325A078.pf | C:/Windows/Prefetch\AUTOMODEDETECT.EXE-0325A078.pf | exe=AUTOMODEDETECT.EXE | source=local:poor_billionaire, pref_hash=325a078, files_count=44, volumes_count=1	
2025-12-09T14:19:31.734142Z	prefetch	[Session 243] ■ Executed Program (runs: 0) AUTOMODEDETECT.EXE-0325A078.pf | C:/Windows/Prefetch\AUTOMODEDETECT.EXE-0325A078.pf | exe=AUTOMODEDETECT.EXE | source=local:poor_billionaire, pref_hash=325a078, files_count=44, volumes_count=1	
2025-12-09T14:19:31.734142Z	prefetch	[Session 243] ■ Executed Program (runs: 0) AUTOMODEDETECT.EXE-0325A078.pf | C:/Windows/Prefetch\AUTOMODEDETECT.EXE-0325A078.pf | exe=AUTOMODEDETECT.EXE | source=local:poor_billionaire, pref_hash=325a078, files_count=44, volumes_count=1	
2025-12-09T14:19:31.754658Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DAX3API.EXE-BEBE53D9.pf | C:/Windows/Prefetch\DAX3API.EXE-BEBE53D9.pf | exe=DAX3API.EXE | source=local:poor_billionaire, pref_hash=bebe53d9, files_count=39, volumes_count=1	
2025-12-09T14:19:31.754658Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DAX3API.EXE-BEBE53D9.pf | C:/Windows/Prefetch\DAX3API.EXE-BEBE53D9.pf | exe=DAX3API.EXE | source=local:poor_billionaire, pref_hash=bebe53d9, files_count=39, volumes_count=1	
2025-12-09T14:19:31.754658Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DAX3API.EXE-BEBE53D9.pf | C:/Windows/Prefetch\DAX3API.EXE-BEBE53D9.pf | exe=DAX3API.EXE | source=local:poor_billionaire, pref_hash=bebe53d9, files_count=39, volumes_count=1	
2025-12-09T14:20:09.817853Z	prefetch	[Session 243] ■ Executed Program (runs: 4) CROSSDEVICESERVICE.EXE-8451C51C.pf | C:/Windows/Prefetch\CROSSDEVICESERVICE.EXE-8451C51C.pf | exe=CROSSDEVICESERVICE.EXE | source=local:poor_billionaire, pref_hash=8451c51c, files_count=363, volumes_count=1	
2025-12-09T14:20:09.817853Z	prefetch	[Session 243] ■ Executed Program (runs: 4) CROSSDEVICESERVICE.EXE-8451C51C.pf | C:/Windows/Prefetch\CROSSDEVICESERVICE.EXE-8451C51C.pf | exe=CROSSDEVICESERVICE.EXE | source=local:poor_billionaire, pref_hash=8451c51c, files_count=363, volumes_count=1	
2025-12-09T14:20:09.817853Z	prefetch	[Session 243] ■ Executed Program (runs: 4) CROSSDEVICESERVICE.EXE-8451C51C.pf | C:/Windows/Prefetch\CROSSDEVICESERVICE.EXE-8451C51C.pf | exe=CROSSDEVICESERVICE.EXE | source=local:poor_billionaire, pref_hash=8451c51c, files_count=363, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T14:20:25.046406Z	prefetch	[Session 243] ■ Executed Program (runs: 2) APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | C:/Windows/Prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | exe=APPLICATIONFRAMEHOST.EXE | source=local:poor_billionaire, pref_hash=8ce9a1ee, files_count=111, volumes_count=1	
2025-12-09T14:20:25.046406Z	prefetch	[Session 243] ■ Executed Program (runs: 2) APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | C:/Windows/Prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | exe=APPLICATIONFRAMEHOST.EXE | source=local:poor_billionaire, pref_hash=8ce9a1ee, files_count=111, volumes_count=1	
2025-12-09T14:20:25.046406Z	prefetch	[Session 243] ■ Executed Program (runs: 2) APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | C:/Windows/Prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf | exe=APPLICATIONFRAMEHOST.EXE | source=local:poor_billionaire, pref_hash=8ce9a1ee, files_count=111, volumes_count=1	
2025-12-09T14:20:51.249051Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DLLHOST.EXE-236AEA34.pf | C:/Windows/Prefetch\DLLHOST.EXE-236AEA34.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=236aea34, files_count=29, volumes_count=1	
2025-12-09T14:20:51.249051Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DLLHOST.EXE-236AEA34.pf | C:/Windows/Prefetch\DLLHOST.EXE-236AEA34.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=236aea34, files_count=29, volumes_count=1	
2025-12-09T14:20:51.249051Z	prefetch	[Session 243] ■ Executed Program (runs: 0) DLLHOST.EXE-236AEA34.pf | C:/Windows/Prefetch\DLLHOST.EXE-236AEA34.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=236aea34, files_count=29, volumes_count=1	

Session 244 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T14:30:03.568249Z	prefetch	[Session 244] ■ Executed Program (runs: 4) APPACTIONS.EXE-B02F2028.pf | C:/Windows/Prefetch\APPACTIONS.EXE-B02F2028.pf | exe=APPACTIONS.EXE | source=local:poor_billionaire, pref_hash=b02f2028, files_count=96, volumes_count=1	
2025-12-09T14:30:03.568249Z	prefetch	[Session 244] ■ Executed Program (runs: 4) APPACTIONS.EXE-B02F2028.pf | C:/Windows/Prefetch\APPACTIONS.EXE-B02F2028.pf | exe=APPACTIONS.EXE | source=local:poor_billionaire, pref_hash=b02f2028, files_count=96, volumes_count=1	
2025-12-09T14:30:03.568249Z	prefetch	[Session 244] ■ Executed Program (runs: 4) APPACTIONS.EXE-B02F2028.pf | C:/Windows/Prefetch\APPACTIONS.EXE-B02F2028.pf | exe=APPACTIONS.EXE | source=local:poor_billionaire, pref_hash=b02f2028, files_count=96, volumes_count=1	

Session 245 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T14:35:36.288606Z	prefetch	[Session 245] ■ Executed Program (runs: 0) BGHELPER.EXE-719117EE.pf | C:/Windows/Prefetch\BGHELPER.EXE-719117EE.pf | exe=BGHELPER.EXE | source=local:poor_billionaire, pref_hash=719117ee, files_count=42, volumes_count=1	
2025-12-09T14:35:36.288606Z	prefetch	[Session 245] ■ Executed Program (runs: 0) BGHELPER.EXE-719117EE.pf | C:/Windows/Prefetch\BGHELPER.EXE-719117EE.pf | exe=BGHELPER.EXE | source=local:poor_billionaire, pref_hash=719117ee, files_count=42, volumes_count=1	
2025-12-09T14:35:36.288606Z	prefetch	[Session 245] ■ Executed Program (runs: 0) BGHELPER.EXE-719117EE.pf | C:/Windows/Prefetch\BGHELPER.EXE-719117EE.pf | exe=BGHELPER.EXE | source=local:poor_billionaire, pref_hash=719117ee, files_count=42, volumes_count=1	

Session 246 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T14:43:48.893241Z	prefetch	[Session 246] ■ Executed Program (runs: 0) DEFRAG.EXE-3D9E8D72.pf | C:/Windows/Prefetch\DEFRAG.EXE-3D9E8D72.pf | exe=DEFRAG.EXE | source=local:poor_billionaire, pref_hash=3d9e8d72, files_count=27, volumes_count=1	
2025-12-09T14:43:48.893241Z	prefetch	[Session 246] ■ Executed Program (runs: 0) DEFRAG.EXE-3D9E8D72.pf | C:/Windows/Prefetch\DEFRAG.EXE-3D9E8D72.pf | exe=DEFRAG.EXE | source=local:poor_billionaire, pref_hash=3d9e8d72, files_count=27, volumes_count=1	
2025-12-09T14:43:48.893241Z	prefetch	[Session 246] ■ Executed Program (runs: 0) DEFRAG.EXE-3D9E8D72.pf | C:/Windows/Prefetch\DEFRAG.EXE-3D9E8D72.pf | exe=DEFRAG.EXE | source=local:poor_billionaire, pref_hash=3d9e8d72, files_count=27, volumes_count=1	

Session 247 — 35 event(s)

Time	Type	Detail	Anomaly
2025-12-09T15:26:58.331120Z	prefetch	[Session 247] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3DB.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DB.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3db, files_count=355, volumes_count=1	
2025-12-09T15:26:58.331120Z	prefetch	[Session 247] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3DB.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DB.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3db, files_count=355, volumes_count=1	
2025-12-09T15:26:58.331120Z	prefetch	[Session 247] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3DB.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DB.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3db, files_count=355, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T15:27:00.061896Z	prefetch	[Session 247] ■ Executed Program (runs: 0) COMPPKGSRV.EXE-4780F0C1.pf | C:/Windows/Prefetch\COMPPKGSRV.EXE-4780F0C1.pf | exe=COMPPKGSRV.EXE | source=local:poor_billionaire, pref_hash=4780f0c1, files_count=30, volumes_count=1	
2025-12-09T15:27:00.061896Z	prefetch	[Session 247] ■ Executed Program (runs: 0) COMPPKGSRV.EXE-4780F0C1.pf | C:/Windows/Prefetch\COMPPKGSRV.EXE-4780F0C1.pf | exe=COMPPKGSRV.EXE | source=local:poor_billionaire, pref_hash=4780f0c1, files_count=30, volumes_count=1	
2025-12-09T15:27:00.061896Z	prefetch	[Session 247] ■ Executed Program (runs: 0) COMPPKGSRV.EXE-4780F0C1.pf | C:/Windows/Prefetch\COMPPKGSRV.EXE-4780F0C1.pf | exe=COMPPKGSRV.EXE | source=local:poor_billionaire, pref_hash=4780f0c1, files_count=30, volumes_count=1	
2025-12-09T15:27:56.949135Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DF.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DF.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3df, files_count=33, volumes_count=1	
2025-12-09T15:27:56.949135Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DF.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DF.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3df, files_count=33, volumes_count=1	
2025-12-09T15:27:56.949135Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DF.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DF.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3df, files_count=33, volumes_count=1	
2025-12-09T15:27:57.108400Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DD.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DD.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dd, files_count=112, volumes_count=1	
2025-12-09T15:27:57.108400Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DD.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DD.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dd, files_count=112, volumes_count=1	
2025-12-09T15:27:57.108400Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DD.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DD.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dd, files_count=112, volumes_count=1	
2025-12-09T15:27:57.116186Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E6.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E6.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e6, files_count=257, volumes_count=1	
2025-12-09T15:27:57.116186Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E6.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E6.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e6, files_count=257, volumes_count=1	
2025-12-09T15:27:57.116186Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E6.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E6.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e6, files_count=257, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T15:27:57.145529Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E8.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E8.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e8, files_count=78, volumes_count=1	
2025-12-09T15:27:57.145529Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E8.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E8.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e8, files_count=78, volumes_count=1	
2025-12-09T15:27:57.145529Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E8.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E8.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e8, files_count=78, volumes_count=1	
2025-12-09T15:28:00.794535Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E7.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E7.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e7, files_count=66, volumes_count=1	
2025-12-09T15:28:00.794535Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E7.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E7.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e7, files_count=66, volumes_count=1	
2025-12-09T15:28:00.794535Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E7.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E7.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e7, files_count=66, volumes_count=1	
2025-12-09T15:28:42.324760Z	shellbag	[Session 247] ■ Folder Viewed artifacts-parser-v1.2.1 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.1 | source=registry	
2025-12-09T15:29:24.700000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $I7DQ6RT.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I7DQ6RT.pdf	
2025-12-09T15:29:24.700000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $I7DQ6RT.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$I7DQ6RT.pdf	
2025-12-09T15:29:24.702000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IMZLPJC.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IMZLPJC.pdf	
2025-12-09T15:29:24.702000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IMZLPJC.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IMZLPJC.pdf	
2025-12-09T15:29:24.704000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IRFVGH6.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IRFVGH6.pdf	
2025-12-09T15:29:24.704000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IRFVGH6.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IRFVGH6.pdf	
2025-12-09T15:29:24.706000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IY652VT.csv \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IY652VT.csv	
2025-12-09T15:29:24.706000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IY652VT.csv \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IY652VT.csv	

Time	Type	Detail	Anomaly
2025-12-09T15:29:24.708000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IB8ZN1M.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IB8ZN1M.pdf	
2025-12-09T15:29:24.708000Z	recycle_i	[Session 247] ■ Recycle Bin (deleted file) $IB8ZN1M.pdf \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IB8ZN1M.pdf	
2025-12-09T15:29:57.122187Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E5.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E5.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e5, files_count=99, volumes_count=1	
2025-12-09T15:29:57.122187Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E5.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E5.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e5, files_count=99, volumes_count=1	
2025-12-09T15:29:57.122187Z	prefetch	[Session 247] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3E5.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E5.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e5, files_count=99, volumes_count=1	

Session 248 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T15:32:09.258592Z	shellbag	[Session 248] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.1\artifacts-parser\@ | source=registry	
2025-12-09T15:32:54.034306Z	shellbag	[Session 248] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.1\artifacts-parser | source=registry	
2025-12-09T15:32:54.034306Z	shellbag	[Session 248] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.1\artifacts-parser\■ | source=registry	

Session 249 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T15:43:10.267416Z	shellbag	[Session 249] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.1.3\artifacts-parser | source=registry	

Session 250 — 2 event(s)

Time	Type	Detail	Anomaly
2025-12-09T15:47:54.141574Z	shellbag	[Session 250] ■ Folder Viewed artifacts-parser-v1.2.3 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.3 | source=registry	
2025-12-09T15:47:55.501616Z	shellbag	[Session 250] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.3\artifacts-parser\@ | source=registry	

Session 251 — 17 event(s)

Time	Type	Detail	Anomaly
2025-12-09T15:55:55.866000Z	recycle_i	[Session 251] ■ Recycle Bin (deleted file) $IKIYUYK.zip \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IKIYUYK.zip	
2025-12-09T15:55:55.866000Z	recycle_i	[Session 251] ■ Recycle Bin (deleted file) $IKIYUYK.zip \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IKIYUYK.zip	
2025-12-09T15:55:57.036742Z	shellbag	[Session 251] ■ Folder Viewed Forensics.v.1.0.4 | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.3\artifacts-parser\Forensics.v.1.0.4 | source=registry	
2025-12-09T15:56:00.452677Z	prefetch	[Session 251] ■ Executed Program (runs: 3) CONSENT.EXE-40419367.pf | C:/Windows/Prefetch\CONSENT.EXE-40419367.pf | exe=CONSENT.EXE | source=local:poor_billionaire, pref_hash=40419367, files_count=175, volumes_count=2	
2025-12-09T15:56:00.452677Z	prefetch	[Session 251] ■ Executed Program (runs: 3) CONSENT.EXE-40419367.pf | C:/Windows/Prefetch\CONSENT.EXE-40419367.pf | exe=CONSENT.EXE | source=local:poor_billionaire, pref_hash=40419367, files_count=175, volumes_count=2	
2025-12-09T15:56:00.452677Z	prefetch	[Session 251] ■ Executed Program (runs: 3) CONSENT.EXE-40419367.pf | C:/Windows/Prefetch\CONSENT.EXE-40419367.pf | exe=CONSENT.EXE | source=local:poor_billionaire, pref_hash=40419367, files_count=175, volumes_count=2	
2025-12-09T15:56:13.402523Z	prefetch	[Session 251] ■ Executed Program (runs: 0) COMPATTELRUNNER.EXE-B7A68ECC.pf | C:/Windows/Prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf | exe=COMPATTELRUNNER.EXE | source=local:poor_billionaire, pref_hash=b7a68ecc, files_count=19, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T15:56:13.402523Z	prefetch	[Session 251] ■ Executed Program (runs: 0) COMPATTELRUNNER.EXE-B7A68ECC.pf | C:/Windows/Prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf | exe=COMPATTELRUNNER.EXE | source=local:poor_billionaire, pref_hash=b7a68ecc, files_count=19, volumes_count=1	
2025-12-09T15:56:13.402523Z	prefetch	[Session 251] ■ Executed Program (runs: 0) COMPATTELRUNNER.EXE-B7A68ECC.pf | C:/Windows/Prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf | exe=COMPATTELRUNNER.EXE | source=local:poor_billionaire, pref_hash=b7a68ecc, files_count=19, volumes_count=1	
2025-12-09T15:56:28.501003Z	prefetch	[Session 251] ■ Executed Program (runs: 7) DLLHOST.EXE-8B4C8C25.pf | C:/Windows/Prefetch\DLLHOST.EXE-8B4C8C25.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=8b4c8c25, files_count=87, volumes_count=1	
2025-12-09T15:56:28.501003Z	prefetch	[Session 251] ■ Executed Program (runs: 7) DLLHOST.EXE-8B4C8C25.pf | C:/Windows/Prefetch\DLLHOST.EXE-8B4C8C25.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=8b4c8c25, files_count=87, volumes_count=1	
2025-12-09T15:56:28.501003Z	prefetch	[Session 251] ■ Executed Program (runs: 7) DLLHOST.EXE-8B4C8C25.pf | C:/Windows/Prefetch\DLLHOST.EXE-8B4C8C25.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=8b4c8c25, files_count=87, volumes_count=1	
2025-12-09T15:56:31.052102Z	prefetch	[Session 251] ■ Executed Program (runs: 4) DLLHOST.EXE-45076844.pf | C:/Windows/Prefetch\DLLHOST.EXE-45076844.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=45076844, files_count=39, volumes_count=1	
2025-12-09T15:56:31.052102Z	prefetch	[Session 251] ■ Executed Program (runs: 4) DLLHOST.EXE-45076844.pf | C:/Windows/Prefetch\DLLHOST.EXE-45076844.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=45076844, files_count=39, volumes_count=1	
2025-12-09T15:56:31.052102Z	prefetch	[Session 251] ■ Executed Program (runs: 4) DLLHOST.EXE-45076844.pf | C:/Windows/Prefetch\DLLHOST.EXE-45076844.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=45076844, files_count=39, volumes_count=1	
2025-12-09T15:57:18.504000Z	recycle_i	[Session 251] ■ Recycle Bin (deleted file) $IFO409C.4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IFO409C.4	
2025-12-09T15:57:18.504000Z	recycle_i	[Session 251] ■ Recycle Bin (deleted file) $IFO409C.4 \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IFO409C.4	

Session 252 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T16:03:20.919135Z	prefetch	[Session 252] ■ Executed Program (runs: 0) BRAVEUPDATE.EXE-71F336A7.pf | C:/Windows/Prefetch\BRAVEUPDATE.EXE-71F336A7.pf | exe=BRAVEUPDATE.EXE | source=local:poor_billionaire, pref_hash=71f336a7, files_count=92, volumes_count=1	
2025-12-09T16:03:20.919135Z	prefetch	[Session 252] ■ Executed Program (runs: 0) BRAVEUPDATE.EXE-71F336A7.pf | C:/Windows/Prefetch\BRAVEUPDATE.EXE-71F336A7.pf | exe=BRAVEUPDATE.EXE | source=local:poor_billionaire, pref_hash=71f336a7, files_count=92, volumes_count=1	
2025-12-09T16:03:20.919135Z	prefetch	[Session 252] ■ Executed Program (runs: 0) BRAVEUPDATE.EXE-71F336A7.pf | C:/Windows/Prefetch\BRAVEUPDATE.EXE-71F336A7.pf | exe=BRAVEUPDATE.EXE | source=local:poor_billionaire, pref_hash=71f336a7, files_count=92, volumes_count=1	

Session 253 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T16:22:31.954624Z	prefetch	[Session 253] ■ Executed Program (runs: 1) CTFMON.EXE-795F8130.pf | C:/Windows/Prefetch\CTFMON.EXE-795F8130.pf | exe=CTFMON.EXE | source=local:poor_billionaire, pref_hash=795f8130, files_count=174, volumes_count=1	
2025-12-09T16:22:31.954624Z	prefetch	[Session 253] ■ Executed Program (runs: 1) CTFMON.EXE-795F8130.pf | C:/Windows/Prefetch\CTFMON.EXE-795F8130.pf | exe=CTFMON.EXE | source=local:poor_billionaire, pref_hash=795f8130, files_count=174, volumes_count=1	
2025-12-09T16:22:31.954624Z	prefetch	[Session 253] ■ Executed Program (runs: 1) CTFMON.EXE-795F8130.pf | C:/Windows/Prefetch\CTFMON.EXE-795F8130.pf | exe=CTFMON.EXE | source=local:poor_billionaire, pref_hash=795f8130, files_count=174, volumes_count=1	

Session 254 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T18:21:24.238498Z	shellbag	[Session 254] ■ Folder Viewed @ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@ | source=registry	

Session 255 — 1 event(s)

Time	Type	Detail	Anomaly
2025-12-09T18:23:28.393594Z	shellbag	[Session 255] ■ Folder Viewed .BIN | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\.BIN | source=registry	

Session 256 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T18:33:17.428551Z	prefetch	[Session 256] ■ Executed Program (runs: 4) AIMGR.EXE-815BA720.pf | C:/Windows/Prefetch\AIMGR.EXE-815BA720.pf | exe=AIMGR.EXE | source=local:poor_billionaire, pref_hash=815ba720, files_count=85, volumes_count=1	
2025-12-09T18:33:17.428551Z	prefetch	[Session 256] ■ Executed Program (runs: 4) AIMGR.EXE-815BA720.pf | C:/Windows/Prefetch\AIMGR.EXE-815BA720.pf | exe=AIMGR.EXE | source=local:poor_billionaire, pref_hash=815ba720, files_count=85, volumes_count=1	
2025-12-09T18:33:17.428551Z	prefetch	[Session 256] ■ Executed Program (runs: 4) AIMGR.EXE-815BA720.pf | C:/Windows/Prefetch\AIMGR.EXE-815BA720.pf | exe=AIMGR.EXE | source=local:poor_billionaire, pref_hash=815ba720, files_count=85, volumes_count=1	

Session 257 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T18:41:13.390971Z	prefetch	[Session 257] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-229CA4CA.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-229CA4CA.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=229ca4ca, files_count=101, volumes_count=1	
2025-12-09T18:41:13.390971Z	prefetch	[Session 257] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-229CA4CA.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-229CA4CA.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=229ca4ca, files_count=101, volumes_count=1	
2025-12-09T18:41:13.390971Z	prefetch	[Session 257] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-229CA4CA.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-229CA4CA.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=229ca4ca, files_count=101, volumes_count=1	

Session 258 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T19:20:29.765537Z	prefetch	[Session 258] ■ Executed Program (runs: 0) AUDIODG.EXE-AB22E9A6.pf | C:/Windows/Prefetch\AUDIODG.EXE-AB22E9A6.pf | exe=AUDIODG.EXE | source=local:poor_billionaire, pref_hash=ab22e9a6, files_count=50, volumes_count=1	
2025-12-09T19:20:29.765537Z	prefetch	[Session 258] ■ Executed Program (runs: 0) AUDIODG.EXE-AB22E9A6.pf | C:/Windows/Prefetch\AUDIODG.EXE-AB22E9A6.pf | exe=AUDIODG.EXE | source=local:poor_billionaire, pref_hash=ab22e9a6, files_count=50, volumes_count=1	
2025-12-09T19:20:29.765537Z	prefetch	[Session 258] ■ Executed Program (runs: 0) AUDIODG.EXE-AB22E9A6.pf | C:/Windows/Prefetch\AUDIODG.EXE-AB22E9A6.pf | exe=AUDIODG.EXE | source=local:poor_billionaire, pref_hash=ab22e9a6, files_count=50, volumes_count=1	

Session 259 — 16 event(s)

Time	Type	Detail	Anomaly
2025-12-09T19:24:21.852364Z	shellbag	[Session 259] ■ Folder Viewed artifacts-parser | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.3\artifacts-parser | source=registry	
2025-12-09T19:24:21.852364Z	shellbag	[Session 259] ■ Folder Viewed ■ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\@\artifacts-parser-v1.2.3\artifacts-parser\■ | source=registry	

Time	Type	Detail	Anomaly
2025-12-09T19:25:23.285383Z	prefetch	[Session 259] ■ Executed Program (runs: 3) CODE.EXE-D24325FA.pf | C:/Windows/Prefetch\CODE.EXE-D24325FA.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fa, files_count=367, volumes_count=2	
2025-12-09T19:25:23.285383Z	prefetch	[Session 259] ■ Executed Program (runs: 3) CODE.EXE-D24325FA.pf | C:/Windows/Prefetch\CODE.EXE-D24325FA.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fa, files_count=367, volumes_count=2	
2025-12-09T19:25:23.285383Z	prefetch	[Session 259] ■ Executed Program (runs: 3) CODE.EXE-D24325FA.pf | C:/Windows/Prefetch\CODE.EXE-D24325FA.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fa, files_count=367, volumes_count=2	
2025-12-09T19:26:01.503049Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-429F6DB6.pf | C:/Windows/Prefetch\DLLHOST.EXE-429F6DB6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=429f6db6, files_count=55, volumes_count=1	
2025-12-09T19:26:01.503049Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-429F6DB6.pf | C:/Windows/Prefetch\DLLHOST.EXE-429F6DB6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=429f6db6, files_count=55, volumes_count=1	
2025-12-09T19:26:01.503049Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-429F6DB6.pf | C:/Windows/Prefetch\DLLHOST.EXE-429F6DB6.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=429f6db6, files_count=55, volumes_count=1	
2025-12-09T19:26:01.625277Z	prefetch	[Session 259] ■ Executed Program (runs: 7) DLLHOST.EXE-76F911B5.pf | C:/Windows/Prefetch\DLLHOST.EXE-76F911B5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=76f911b5, files_count=72, volumes_count=1	
2025-12-09T19:26:01.625277Z	prefetch	[Session 259] ■ Executed Program (runs: 7) DLLHOST.EXE-76F911B5.pf | C:/Windows/Prefetch\DLLHOST.EXE-76F911B5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=76f911b5, files_count=72, volumes_count=1	
2025-12-09T19:26:01.625277Z	prefetch	[Session 259] ■ Executed Program (runs: 7) DLLHOST.EXE-76F911B5.pf | C:/Windows/Prefetch\DLLHOST.EXE-76F911B5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=76f911b5, files_count=72, volumes_count=1	
2025-12-09T19:26:02.068377Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-7896B35F.pf | C:/Windows/Prefetch\DLLHOST.EXE-7896B35F.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7896b35f, files_count=58, volumes_count=1	
2025-12-09T19:26:02.068377Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-7896B35F.pf | C:/Windows/Prefetch\DLLHOST.EXE-7896B35F.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7896b35f, files_count=58, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T19:26:02.068377Z	prefetch	[Session 259] ■ Executed Program (runs: 4) DLLHOST.EXE-7896B35F.pf | C:/Windows/Prefetch\DLLHOST.EXE-7896B35F.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7896b35f, files_count=58, volumes_count=1	
2025-12-09T19:26:28.248000Z	recycle_i	[Session 259] ■ Recycle Bin (deleted file) $IQG7IUR.py \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IQG7IUR.py	
2025-12-09T19:26:28.248000Z	recycle_i	[Session 259] ■ Recycle Bin (deleted file) $IQG7IUR.py \| D:/$RECYCLE.BIN\S-1-5-21-509071697-2027520391-1498176977-1001\$IQG7IUR.py	

Session 260 — 3 event(s)

Time	Type	Detail	Anomaly
2025-12-09T19:31:49.239466Z	prefetch	[Session 260] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3E9.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E9.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e9, files_count=216, volumes_count=1	
2025-12-09T19:31:49.239466Z	prefetch	[Session 260] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3E9.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E9.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e9, files_count=216, volumes_count=1	
2025-12-09T19:31:49.239466Z	prefetch	[Session 260] ■ Executed Program (runs: 3) BRAVE.EXE-3118B3E9.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3E9.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3e9, files_count=216, volumes_count=1	

Session 261 — 37 event(s)

Time	Type	Detail	Anomaly
2025-12-09T19:46:51.708164Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FE.pf | C:/Windows/Prefetch\CODE.EXE-D24325FE.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fe, files_count=51, volumes_count=1	
2025-12-09T19:46:51.708164Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FE.pf | C:/Windows/Prefetch\CODE.EXE-D24325FE.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fe, files_count=51, volumes_count=1	
2025-12-09T19:46:51.708164Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FE.pf | C:/Windows/Prefetch\CODE.EXE-D24325FE.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fe, files_count=51, volumes_count=1	
2025-12-09T19:46:51.879497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432605.pf | C:/Windows/Prefetch\CODE.EXE-D2432605.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432605, files_count=79, volumes_count=1	
2025-12-09T19:46:51.879497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432605.pf | C:/Windows/Prefetch\CODE.EXE-D2432605.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432605, files_count=79, volumes_count=1	
2025-12-09T19:46:51.879497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432605.pf | C:/Windows/Prefetch\CODE.EXE-D2432605.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432605, files_count=79, volumes_count=1	
2025-12-09T19:46:51.880497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FC.pf | C:/Windows/Prefetch\CODE.EXE-D24325FC.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fc, files_count=96, volumes_count=1	
2025-12-09T19:46:51.880497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FC.pf | C:/Windows/Prefetch\CODE.EXE-D24325FC.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fc, files_count=96, volumes_count=1	
2025-12-09T19:46:51.880497Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FC.pf | C:/Windows/Prefetch\CODE.EXE-D24325FC.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fc, files_count=96, volumes_count=1	
2025-12-09T19:46:52.060555Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FB.pf | C:/Windows/Prefetch\CODE.EXE-D24325FB.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fb, files_count=103, volumes_count=1	
2025-12-09T19:46:52.060555Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FB.pf | C:/Windows/Prefetch\CODE.EXE-D24325FB.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fb, files_count=103, volumes_count=1	
2025-12-09T19:46:52.060555Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D24325FB.pf | C:/Windows/Prefetch\CODE.EXE-D24325FB.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d24325fb, files_count=103, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T19:46:53.990547Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CMD.EXE-0BD30981.pf | C:/Windows/Prefetch\CMD.EXE-0BD30981.pf | exe=CMD.EXE | source=local:poor_billionaire, pref_hash=bd30981, files_count=13, volumes_count=1	
2025-12-09T19:46:53.990547Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CMD.EXE-0BD30981.pf | C:/Windows/Prefetch\CMD.EXE-0BD30981.pf | exe=CMD.EXE | source=local:poor_billionaire, pref_hash=bd30981, files_count=13, volumes_count=1	
2025-12-09T19:46:53.990547Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CMD.EXE-0BD30981.pf | C:/Windows/Prefetch\CMD.EXE-0BD30981.pf | exe=CMD.EXE | source=local:poor_billionaire, pref_hash=bd30981, files_count=13, volumes_count=1	
2025-12-09T19:46:53.997084Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CONHOST.EXE-0C6456FB.pf | C:/Windows/Prefetch\CONHOST.EXE-0C6456FB.pf | exe=CONHOST.EXE | source=local:poor_billionaire, pref_hash=c6456fb, files_count=26, volumes_count=1	
2025-12-09T19:46:53.997084Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CONHOST.EXE-0C6456FB.pf | C:/Windows/Prefetch\CONHOST.EXE-0C6456FB.pf | exe=CONHOST.EXE | source=local:poor_billionaire, pref_hash=c6456fb, files_count=26, volumes_count=1	
2025-12-09T19:46:53.997084Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CONHOST.EXE-0C6456FB.pf | C:/Windows/Prefetch\CONHOST.EXE-0C6456FB.pf | exe=CONHOST.EXE | source=local:poor_billionaire, pref_hash=c6456fb, files_count=26, volumes_count=1	
2025-12-09T19:46:54.816287Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE-TUNNEL.EXE-1CAD4A12.pf | C:/Windows/Prefetch\CODE-TUNNEL.EXE-1CAD4A12.pf | exe=CODE-TUNNEL.EXE | source=local:poor_billionaire, pref_hash=1cad4a12, files_count=43, volumes_count=1	
2025-12-09T19:46:54.816287Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE-TUNNEL.EXE-1CAD4A12.pf | C:/Windows/Prefetch\CODE-TUNNEL.EXE-1CAD4A12.pf | exe=CODE-TUNNEL.EXE | source=local:poor_billionaire, pref_hash=1cad4a12, files_count=43, volumes_count=1	
2025-12-09T19:46:54.816287Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE-TUNNEL.EXE-1CAD4A12.pf | C:/Windows/Prefetch\CODE-TUNNEL.EXE-1CAD4A12.pf | exe=CODE-TUNNEL.EXE | source=local:poor_billionaire, pref_hash=1cad4a12, files_count=43, volumes_count=1	
2025-12-09T19:48:37.237370Z	prefetch	[Session 261] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DC.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DC.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dc, files_count=52, volumes_count=1	
2025-12-09T19:48:37.237370Z	prefetch	[Session 261] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DC.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DC.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dc, files_count=52, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T19:48:37.237370Z	prefetch	[Session 261] ■ Executed Program (runs: 0) BRAVE.EXE-3118B3DC.pf | C:/Windows/Prefetch\BRAVE.EXE-3118B3DC.pf | exe=BRAVE.EXE | source=local:poor_billionaire, pref_hash=3118b3dc, files_count=52, volumes_count=1	
2025-12-09T19:49:52.906611Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432604.pf | C:/Windows/Prefetch\CODE.EXE-D2432604.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432604, files_count=101, volumes_count=1	
2025-12-09T19:49:52.906611Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432604.pf | C:/Windows/Prefetch\CODE.EXE-D2432604.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432604, files_count=101, volumes_count=1	
2025-12-09T19:49:52.906611Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432604.pf | C:/Windows/Prefetch\CODE.EXE-D2432604.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432604, files_count=101, volumes_count=1	
2025-12-09T19:51:21.161598Z	prefetch	[Session 261] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=cad1df16, files_count=76, volumes_count=1	
2025-12-09T19:51:21.161598Z	prefetch	[Session 261] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=cad1df16, files_count=76, volumes_count=1	
2025-12-09T19:51:21.161598Z	prefetch	[Session 261] ■ Executed Program (runs: 4) BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | C:/Windows/Prefetch\BACKGROUNDTASKHOST.EXE-CAD1DF16.pf | exe=BACKGROUNDTASKHOST.EXE | source=local:poor_billionaire, pref_hash=cad1df16, files_count=76, volumes_count=1	
2025-12-09T19:52:27.577502Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432608.pf | C:/Windows/Prefetch\CODE.EXE-D2432608.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432608, files_count=577, volumes_count=1	
2025-12-09T19:52:27.577502Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432608.pf | C:/Windows/Prefetch\CODE.EXE-D2432608.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432608, files_count=577, volumes_count=1	
2025-12-09T19:52:27.577502Z	prefetch	[Session 261] ■ Executed Program (runs: 0) CODE.EXE-D2432608.pf | C:/Windows/Prefetch\CODE.EXE-D2432608.pf | exe=CODE.EXE | source=local:poor_billionaire, pref_hash=d2432608, files_count=577, volumes_count=1	
2025-12-09T19:52:29.111965Z	prefetch	[Session 261] ■ Executed Program (runs: 7) DLLHOST.EXE-A45C43E5.pf | C:/Windows/Prefetch\DLLHOST.EXE-A45C43E5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=a45c43e5, files_count=53, volumes_count=1	

Time	Type	Detail	Anomaly
2025-12-09T19:52:29.111965Z	prefetch	[Session 261] ■ Executed Program (runs: 7) DLLHOST.EXE-A45C43E5.pf | C:/Windows/Prefetch\DLLHOST.EXE-A45C43E5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=a45c43e5, files_count=53, volumes_count=1	
2025-12-09T19:52:29.111965Z	prefetch	[Session 261] ■ Executed Program (runs: 7) DLLHOST.EXE-A45C43E5.pf | C:/Windows/Prefetch\DLLHOST.EXE-A45C43E5.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=a45c43e5, files_count=53, volumes_count=1	
2025-12-09T19:52:48.710203Z	prefetch	[Session 261] ■ Executed Program (runs: 0) DLLHOST.EXE-7D5CE0CA.pf | C:/Windows/Prefetch\DLLHOST.EXE-7D5CE0CA.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7d5ce0ca, files_count=45, volumes_count=2	

Session 262 — 5 event(s)

Time	Type	Detail	Anomaly
2025-12-09T19:57:21.820400Z	prefetch	[Session 262] ■ Executed Program (runs: 0) DLLHOST.EXE-7D5CE0CA.pf | C:/Windows/Prefetch\DLLHOST.EXE-7D5CE0CA.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7d5ce0ca, files_count=45, volumes_count=2	
2025-12-09T19:57:21.820400Z	prefetch	[Session 262] ■ Executed Program (runs: 0) DLLHOST.EXE-7D5CE0CA.pf | C:/Windows/Prefetch\DLLHOST.EXE-7D5CE0CA.pf | exe=DLLHOST.EXE | source=local:poor_billionaire, pref_hash=7d5ce0ca, files_count=45, volumes_count=2	
2025-12-09T19:57:25.947768Z	shellbag	[Session 262] ■ Folder Viewed C:\ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\C:\ | source=registry	
2025-12-09T19:58:32.686260Z	shellbag	[Session 262] ■ Folder Viewed {E04FD020EA3A6910A2D808002B30309D} | CLSID\{E04FD020EA3A6910A2D808002B30309D} | source=registry	
2025-12-09T19:58:32.838806Z	shellbag	[Session 262] ■ Folder Viewed D:\ | CLSID\{E04FD020EA3A6910A2D808002B30309D}\D:\ | source=registry	

Note: Events grouped into sessions by time gaps (parser logic). Export contains full DB for detailed artifact review.