```
{
 "_index": ".ds-logs-filestream.generic-cowrie-2026.01.28-000001",
 "_id": "AZwGdAPtV5wNIakYI_MC",
 "_version": 1,
 "_source": {
  "@timestamp": "2026-01-28T21:13:06.309Z",
  "agent": {
   "ephemeral_id": "979ea20c-99a0-4073-b5d7-36dec8646159",
   "id": "7a33f160-d194-4cbb-b927-6ac5597a473d",
   "name": "kali",
   "type": "filebeat",
   "version": "9.2.4"
  },
  "data_stream": {
   "dataset": "filestream.generic",
   "namespace": "cowrie",
   "type": "logs"
  },
  "ecs": {
   "version": "8.0.0"
  },
  "elastic_agent": {
   "id": "7a33f160-d194-4cbb-b927-6ac5597a473d",
   "snapshot": false,
   "version": "9.2.4"
  },
  "event": {
   "agent_id_status": "verified",
   "dataset": "filestream.generic",
   "ingested": "2026-01-28T21:13:17Z"
```

```
},
"host": {
  "architecture": "x86_64",
  "containerized": false,
  "hostname": "kali",
  "id": "b69758c0cad3481e967dcad827001d56",
  "ip": [
    "192.168.200.99",
    "fe80::a628:781e:1d4d:2e15",
    "172.17.0.1",
    "fe80::42:b0ff:fe70:b4a7",
    "fe80::809b:84ff:fe59:73e2"
  ],
  "mac": [
    "02-42-B0-70-B4-A7",
    "08-00-27-63-B0-05",
    "82-9B-84-59-73-E2"
  ],
  "name": "kali",
  "os": {
    "codename": "kali-rolling",
    "family": "debian",
    "kernel": "6.18.5+kali-amd64",
    "name": "Kali GNU/Linux",
    "platform": "kali",
    "type": "linux",
    "version": "2025.4"
  }
},
"input": {
```

```
    "type": "filestream"
   },
   "log": {
    "file": {
     "device_id": "2049",
     "fingerprint": "8bcf86b77af4a6132b23c79937a0f0d95fa1868d19992867bbf184aeb2830d4c",
     "inode": "4198472",
     "path": "/home/kali/logs-cowrie.log"
    },
    "offset": "11204"
   },
   "message": "2026-01-28T21:13:04+0000 [HoneyPotSSHTransport,2,192.168.0.182] Command found: pwd "
  },
  "fields": {
   "elastic_agent.version": [
    "9.2.4"
   ],
   "host.os.name.text": [
    "Kali GNU/Linux"
   ],
   "host.hostname": [
    "kali"
   ],
   "host.mac": [
    "02-42-B0-70-B4-A7",
    "08-00-27-63-B0-05",
    "82-9B-84-59-73-E2"
   ],
   "host.ip": [
    "192.168.200.99",
```

```
    "fe80::a628:781e:1d4d:2e15",
    "172.17.0.1",
    "fe80::42:b0ff:fe70:b4a7",
    "fe80::809b:84ff:fe59:73e2"
  ],
  "agent.type": [
    "filebeat"
  ],
  "event.module": [
    "filestream"
  ],
  "host.os.version": [
    "2025.4"
  ],
  "host.os.kernel": [
    "6.18.5+kali-amd64"
  ],
  "log.file.device_id": [
    "2049"
  ],
  "host.os.name": [
    "Kali GNU/Linux"
  ],
  "agent.name": [
    "kali"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "host.name": [
```

```
    "kali"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "host.id": [
    "b69758c0cad3481e967dcad827001d56"
  ],
  "host.os.type": [
    "linux"
  ],
  "elastic_agent.id": [
    "7a33f160-d194-4cbb-b927-6ac5597a473d"
  ],
  "data_stream.namespace": [
    "cowrie"
  ],
  "host.os.codename": [
    "kali-rolling"
  ],
  "input.type": [
    "filestream"
  ],
  "log.offset": [
    "11204"
  ],
  "message": [
    "2026-01-28T21:13:04+0000 [HoneyPotSSHTransport,2,192.168.0.182] Command found: pwd "
  ],
  "data_stream.type": [
```

```
  "logs"
],
"host.architecture": [
  "x86_64"
],
"event.ingested": [
  "2026-01-28T21:13:17.000Z"
],
"@timestamp": [
  "2026-01-28T21:13:06.309Z"
],
"agent.id": [
  "7a33f160-d194-4cbb-b927-6ac5597a473d"
],
"ecs.version": [
  "8.0.0"
],
"host.containerized": [
  false
],
"host.os.platform": [
  "kali"
],
"log.file.inode": [
  "4198472"
],
"data_stream.dataset": [
  "filestream.generic"
],
"log.file.path": [
```

```
      "/home/kali/logs-cowrie.log"
    ],
    "agent.ephemeral_id": [
      "979ea20c-99a0-4073-b5d7-36dec8646159"
    ],
    "agent.version": [
      "9.2.4"
    ],
    "log.file.fingerprint": [
      "8bcf86b77af4a6132b23c79937a0f0d95fa1868d19992867bbf184aeb2830d4c"
    ],
    "host.os.family": [
      "debian"
    ],
    "event.dataset": [
      "filestream.generic"
    ]
  }
}
```