The Sandbox Report Structure

The sandbox report consolidates the results of static analysis and multiple sandbox analysis for the same file.

The report includes the following fields:

Name	Description
Resource Info	**Includes general information about the submitted file**
resource_type	This field indicates the type of resource: sample
file_size	This field indicates the size of the submitted file
resource	This field indicates the submitted file's hash value
first_seen	This field indicates the time that the file was first submitted to the sandbox
analysis_complete	This field indicates if the analysis was completed (true or false)
file_types	This field indicates the file type/s that were identified during the analysis
resource_md5	This field indicates the md5 of the submitted file
Threat Summary	**Includes information about the file analysis determination**
resource_score	This field indicates the final analysis score. The score is between 0 and 100 (riskiest)
determination_date	This field indicates the time stamp for the file's score calculation
Static Analysis	**Includes the list of risks identified during the static analysis phase and their score**
score	This field indicates the score for the static analysis
risks	This field indicates the list of identified static risks (anti-vm, anti-debugging, anti-sandbox, packers etc), and is used in the selection of the most suitable sandbox
Dynamic Analysis	**Includes the list of behavioral risks identified during the dynamic analysis phase and their score. The risks are divided into operating system activity risks and network activity risks**
OS Activity	**Indicates the risky operating system behaviors identified during the analysis**
behavior	Indicates the list of behaviors
score	This field indicates the combined score for all OS activity behavior risks
risks	This field indicates the list of suspicious and malicious OS activity behavior
dropped_files	Includes a list of risks identified due to download of additional files during the original file's analysis
score	This field indicates if a known malicious file is dropped, or downloaded by the sandbox
risks	This field indicates a list of risks associated with the drop behavior
Network Activity	**Includes the list of network activities**
behavior	This field indicates the behavior
score	This field indicates the combined score for all network activity behaviour risks
risks	This field indicates the list of suspicious and malicious network activity behaviour, based on lists of known malicious urls, and P addresses

Signatures	Includes the list of detected IDS signatures
score	This field indicates the combined score for all network activity signatures
risks	This field indicates the List of signatures (NIMR rules)
Footprint	**Includes a summary of the indicators of compromise that contributed to the overall risk score**
url	This field indicates the suspicious urls contacted during analyses
ip	This field indicates the suspicious IP addresses
ssl_cert_subject	This field indicates the suspicious ssl certificates
file_sha256	This field indicates the suspicious sha256
http_user_agent	This field indicates the suspicious http user agents
Analyses	**Includes the multiple analyses raw data**
analysis_id	This field indicates the unique analysis id. One sample can have many analysis id's
analysis_score	This field indicates the combined score for a sample, which is calculated from resource score, dynamic analysis score and network score
analysis_status	This field indicates the status of the analysis
added_at	This field indicates the timestamp for the current analysis
configuration_description	This field indicates which operating system the file was run on
Activity Report	**Includes the activity report**
OS	This field indicates the OS
Process	This field indicates the list of processes run during analysis, and the $NAME$ indicates the process for the sample itself
file_activity	This field indicates the read, write, store, and delete file activity
process_activity	This field indicates the detailed view of the process activity
service_activity	This field indicates the services that were started, controlled, paused, stopped etc.
registry_activity	This field indicates all the registry activit, which inludes read, set and delete
mutex_activity	This field indicates the list of created and used mutexes
window_activity	This field indicates the list of window activity (search for window, close window etc)
dropped files	This field indicates the metadata fro all dropped files
network	This field indicates the list of all network activity

Sandbox Report Example


```
{
  "resource_info": {
    "resource_type": "sample",
    "file_size": 102185,
    "resource": "71a54a2cd2a6caef8d80aac7a83619ac0cea246a94ee449aca5319b0085bb105",
    "first_seen": "2017-11-07 08:06:24",
    "analysis_complete": true,
    "file_types": [
      "TEXT File"
    ],
    "resource_md5": "1c7bbed7bb232012e400563ec089dda1"
  },
  "threat_summary": {
    "resource_score": 93,
```

```
    "determination_date": "2017-11-08 10:07:38",
    "static_analysis": {
      "score": 0,
      "risks": []
    },
    "dynamic_analysis": {
      "os_activity": {
        "behaviour": {
          "score": 93,
          "risks": [
            {
              "risk": "Creates Mutex",
              "severity": "low",
              "metadata": [
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_idx.db!rwWriterMutex"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_32.db!dfMaintainer"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_96.db!dfMaintainer"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_256.db!dfMaintainer"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_1024.db!dfMaintainer"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_sr.db!dfMaintainer"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_idx.db!ThumbnailCacheInit"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\explorer.exe",
                  "mutex_name": "Global\\C::Users:Patrick:AppData:Local:Microsoft:
Windows:Explorer:thumbcache_idx.db!rwReaderRefs"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "eHomeNameMutex"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Local\\__DDrawExclMode__"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Local\\__DDrawCheckExclMode__"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "DirectSound Administrator shared thread array
(lock)"
                },
                {
```

```
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "RasPbFile"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreOpen_b4cae1f9a3aead62bebb934ca33cadb730c8d3ed"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreSyncMem_5ea381292eeb3ed3e61dc84a3dbd4d7f59767eca"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreSyncMem_7715dc857070a1523dea43f32f1fe67c1ce58e0b"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreSyncMem_71bdfe29063ac557a4e7b3205ed180408457fcd4"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_1"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-
0.db"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-
0.db:x"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-
0.db:splk:1412"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreSyncMem_02004a9f865399b5c2a02973d5e53544ed4ce2ea"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbRWMutex_1"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_2"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{859fbcff-b806-4b7f-860b-f66a3a09232f}:
sqlce_se_lck:1"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreCreateTable_a1d78cdcc411921ce3b07770aa2a0e0745789b11"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{859fbcff-b806-4b7f-860b-f66a3a09232f}:
sqlce_se_lck:2"
```

```
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\MCStoreAddStoredType_a1d78cdcc411921ce3b07770aa2a0e0745789b11"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_3"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_4"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_5"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\MediaCenter.
MCUpdate_7000000000026_a1d78cdcc411921ce3b07770aa2a0e0745789b11"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{859fbcff-b806-4b7f-860b-f66a3a09232f}:
sqlce_se_lck:3"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Local\\MICROSOFT_WMDM_MUTEX"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name":
"Global\\ReinitMCUpdate_a1d78cdcc411921ce3b07770aa2a0e0745789b11"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbRWMutex_2"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_6"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_7"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbRWMutex_3"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\eHome_DbMutex_8"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-
0.db:splk:1428"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{934d67ff-486b-4280-acf6-c1a863190007}:
sqlce_se_lck:1"
                },
                {
                  "action": "mutex created",
```

```
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{934d67ff-486b-4280-acf6-c1a863190007}:
sqlce_se_lck:2"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{934d67ff-486b-4280-acf6-c1a863190007}:
sqlce_se_lck:3"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-
0.db:splk:1944"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:
sqlce_se_lck:1"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:
sqlce_se_lck:2"
                },
                {
                  "action": "mutex created",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "mutex_name": "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:
sqlce_se_lck:3"
                }
              ]
            },
            {
              "risk": "Sleeps for a short time",
              "severity": "low",
              "metadata": []
            },
            {
              "risk": "Sleeps for a medium time",
              "severity": "medium",
              "metadata": []
            },
            {
              "risk": "Sleeps for a very very long time",
              "severity": "high",
              "metadata": []
            },
            {
              "risk": "Searches for Shell TrayWnd",
              "severity": "low",
              "metadata": []
            },
            {
              "risk": "Accesses the Kernel Security Device Driver",
              "severity": "low",
              "metadata": [
                {
                  "action": "file accessed",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "file_name": "\\Device\\KsecDD"
                }
              ]
            },
            {
              "risk": "Allocates executable memory",
              "severity": "low",
              "metadata": [
                {
                  "action": "memory allocated",
                  "process": "C:\\Windows\\ehome\\ehshell.exe",
                  "details": "PAGE_EXECUTE_READWRITE"
                },
                {
                  "action": "memory allocated",
                  "process": "C:\\Windows\\explorer.exe",
                  "details": "PAGE_EXECUTE_READWRITE"
                }
              ]
            },
            {
```

```
              "risk": "Checks for user activity",
              "severity": "low",
              "metadata": []
            },
            {
              "risk": null,
              "severity": "low",
              "metadata": []
            },
            {
              "risk": "Monitors keyboard",
              "severity": "low",
              "metadata": [
                {
                  "action": "hook created",
                  "process": "C:\\Windows\\explorer.exe",
                  "details": "WH_KEYBOARD_LL"
                }
              ]
            }
          ]
        },
        "dropped_files": {
          "score": null,
          "risks": null
        }
      },
      "network_activity": {
        "behaviour": {
          "score": 0,
          "risks": []
        },
        "signatures": {
          "score": 0,
          "risks": []
        }
      }
    }
  },
  "footprint": {
    "url": [],
    "ip": [],
    "ssl_cert_subject": [],
    "file_sha256": [],
    "http_user_agent": []
  },
  "analyses": [
    {
          "analysis_id": 7317,
      "configuration_description": "windows7.professional.32bit",
      "analysis_score": 93,
      "analysis_status": "determined_successfully",
      "added_at": "2017-11-09 10:05:24",
      "activity_report": {
        "os": [
          {
            "process": "C:\\Windows\\System32\\cmd.exe",
            "file_activity": {
              "read_files": [
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Caches\\cversions.1.db",
                "%USERPROFILE%\\AppData\\Local\\Microsoft\\Windows\\Caches\\
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x30x000000000000000b.db",
                "%USERPROFILE%\\Searches\\desktop.ini",
                "%USERPROFILE%\\Videos\\desktop.ini",
                "%USERPROFILE%\\Pictures\\desktop.ini",
                "%USERPROFILE%\\Contacts\\desktop.ini",
                "%USERPROFILE%\\Music\\desktop.ini",
                "%USERPROFILE%\\Links\\desktop.ini",
                "%USERPROFILE%\\Saved Games\\desktop.ini",
                "C:\\Windows\\System32\\rundll32.exe",
                "C:\\Windows\\System32\\cmd.exe",
                "%USERPROFILE%\\Desktop\\desktop.ini",
                "%USERPROFILE%\\Favorites\\desktop.ini",
                "%USERPROFILE%\\Downloads\\desktop.ini",
                "%USERPROFILE%\\Documents\\desktop.ini",
                "C:\\Windows\\System32\\shdocvw.dll",
                "C:\\Windows\\winsxs\\FileMaps\\$$_system32_21f9a9c4a2f8b514.cdf-
ms"
              ]
            },
            "process_activity": {
              "created_processes": [
                {
```

```
                  "file_path": "%USERPROFILE%\\AppData\\Local\\Temp\\$NAME$",
                  "process_arguments": null
                },
                {
                  "file_path": "%USERPROFILE%\\AppData\\Local\\Temp\\$NAME$",
                  "process_arguments": "C:
\\Users\\Patrick\\AppData\\Local\\Temp\\$NAME$ "
                },
                {
                  "file_path": "C:\\Windows\\System32\\rundll32.exe",
                  "process_arguments": "\"C:\\Windows\\system32\\rundll32.exe\" C:
\\Windows\\system32\\shell32.dll,OpenAs_RunDLL C:
\\Users\\$USER$\\AppData\\Local\\Temp\\$NAME$"
                }
              ]
            },
            "service_activity": [],
            "registry_activity": [],
            "mutex_activity": [],
            "window_activity": []
          },
          {
            "process": "C:\\Windows\\System32\\rundll32.exe",
            "file_activity": {
              "read_files": [
                "C:\\Windows\\Globalization\\Sorting\\sortdefault.nls",
                "c:\\Windows\\System32\\imageres.dll",
                "c:\\Windows\\System32\\en-US\\imageres.dll.mui",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Caches\\cversions.1.db",
                "%USERPROFILE%\\AppData\\Local\\Microsoft\\Windows\\Caches\\
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x30x000000000000000b.db",
                "C:\\Windows\\ehome\\ehshell.exe",
                "C:\\Program Files\\desktop.ini",
                "C:\\Program Files\\Internet Explorer\\iexplore.exe",
                "C:\\Windows\\System32\\mspaint.exe",
                "C:\\Windows\\System32\\notepad.exe",
                "C:\\Program Files\\Windows Photo Viewer\\PhotoViewer.dll",
                "C:\\Program Files\\Windows Media Player\\wmplayer.exe",
                "C:\\Program Files\\Windows NT\\Accessories\\wordpad.exe",
                "c:\\program files\\windows nt\\accessories\\wordpad.exe",
                "c:\\program files\\windows photo viewer\\photoviewer.dll",
                "c:\\program files\\windows photo viewer\\en-US\\photoviewer.dll.
mui",
                "c:\\program files\\windows media player\\wmplayer.exe",
                "c:\\program files\\windows media player\\en-US\\wmplayer.exe.mui",
                "c:\\Windows\\ehome\\ehshell.exe",
                "c:\\Windows\\System32\\mspaint.exe",
                "c:\\Windows\\System32\\notepad.exe",
                "c:\\Windows\\System32\\en-US\\notepad.exe.mui",
                "c:\\program files\\internet explorer\\iexplore.exe",
                "c:\\program files\\internet explorer\\en-US\\iexplore.exe.mui",
                "%USERPROFILE%\\AppData\\Local\\Temp",
                "%USERPROFILE%\\Searches\\desktop.ini",
                "%USERPROFILE%\\Videos\\desktop.ini",
                "%USERPROFILE%\\Pictures\\desktop.ini",
                "%USERPROFILE%\\Contacts\\desktop.ini",
                "%USERPROFILE%\\Music\\desktop.ini",
                "%USERPROFILE%\\Links\\desktop.ini",
                "%USERPROFILE%\\Saved Games\\desktop.ini",
                "C:\\Windows\\ehome\\ehshell.exe",
                "C:\\Windows\\System32\\rundll32.exe",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\desktop.ini",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\desktop.ini",
                "C:\\Windows\\System32\\EhStorShell.dll",
                "C:\\Windows\\System32\\cscui.dll",
                "C:\\Windows\\System32\\ntshrui.dll",
                "%USERPROFILE%\\Desktop\\desktop.ini",
                "%USERPROFILE%\\Favorites\\desktop.ini",
                "%USERPROFILE%\\Downloads\\desktop.ini",
                "%USERPROFILE%\\Documents\\desktop.ini",
                "C:\\Windows\\System32\\shdocvw.dll",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\desktop.ini",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\desktop.ini",
                "%USERPROFILE%\\desktop.ini"
              ]
            },
```

```
            "process_activity": {
              "created_processes": [
                {
                  "file_path": "%USERPROFILE%\\AppData\\Local\\Temp\\$NAME$",
                  "process_arguments": null
                },
                {
                  "file_path": "C:\\Windows\\ehome\\ehshell.exe",
                  "process_arguments": "\"C:\\Windows\\eHome\\ehshell.exe\" \"C:
\\Users\\$USER$\\AppData\\Local\\Temp\\$NAME$\""
                }
              ]
            },
            "service_activity": [],
            "registry_activity": {
              "set_values": [
                {
                  "key": "HKEY_CURRENT_USER\\il_auto_file\\(Default)",
                  "value_name": "",
                  "value_set_data": null
                },
                {
                  "key": "HKEY_CURRENT_USER\\.il\\(Default)",
                  "value_name": "il_auto_file",
                  "value_set_data": null
                },
                {
                  "key": "HKEY_CURRENT_USER\\il_auto_file\\shell\\open\\command\\
(Default)",
                  "value_name": "\"C:\\Windows\\eHome\\ehshell.exe\" \"%1\"",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Global
AssocChangedCounter",
                  "value_name": "16",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExt
s\\.il\\OpenWithList\\a",
                  "value_name": "ehshell.exe",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExt
s\\.il\\OpenWithList\\MRUList",
                  "value_name": "a",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExt
s\\.il\\OpenWithProgids\\il_auto_file",
                  "value_name": "",
                  "value_set_data": null
                },
                {
                  "key": "HKEY_CURRENT_USER\\Local
Settings\\MuiCache\\2\\52C64B7E\\LanguageList",
                  "value_name": "en-USu0000enu0000u0000",
                  "value_set_data": null
                }
              ]
            },
            "mutex_activity": {
              "used_mutex": [
                "CicLoadWinStaWinSta0",
                "Local\\MSCTF.CtfMonitorInstMutexDefault1"
              ]
            },
            "window_activity": []
          },
          {
            "process": "C:\\Windows\\explorer.exe",
            "file_activity": {
              "read_files": [
                "%USERPROFILE%\\Desktop\\desktop.ini",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\desktop.ini",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\desktop.ini",
```

```
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_32.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_idx.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_32.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_96.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_256.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_1024.db",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_sr.db",
                "c:\\program files\\windows nt\\accessories\\wordpad.exe",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Internet Explorer.lnk",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Internet Explorer.lnk",
                "C:\\Program Files\\desktop.ini",
                "C:\\Program Files\\Internet Explorer\\iexplore.exe",
                "c:\\program files\\internet explorer\\iexplore.exe",
                "c:\\program files\\internet explorer\\en-US\\iexplore.exe.mui",
                "c:\\Windows\\System32\\imageres.dll",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Windows Explorer.lnk",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Windows Explorer.lnk",
                "C:\\Windows\\explorer.exe",
                "c:\\Windows\\System32\\en-US\\imageres.dll.mui",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Windows Media Player.lnk",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Internet
Explorer\\Quick Launch\\User Pinned\\TaskBar\\Windows Media Player.lnk",
                "C:\\Program Files\\Windows Media Player\\wmplayer.exe",
                "C:\\Program Files\\windows media player\\wmplayer.exe",
                "C:\\Program Files\\windows media player\\en-US\\wmplayer.exe.mui",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Command Prompt.lnk",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Command Prompt.lnk",
                "C:\\Windows\\System32\\cmd.exe",
                "C:\\Windows\\System32\\en-US\\cmd.exe.mui",
                "C:\\ProgramData\\Microsoft\\User Account Pictures\\Patrick.dat",
                "C:\\ProgramData\\Microsoft\\User Account Pictures\\user.bmp",
                "%USERPROFILE%\\desktop.ini",
                "C:
\\Windows\\resources\\Themes\\Aero\\Shell\\NormalColor\\ShellStyle.dll",
                "C:\\Windows\\System32\\imageres.dll",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\Windows\\Start
Menu\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\desktop.ini",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Welcome Center.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Welcome Center.lnk",
                "C:\\Windows\\System32\\rundll32.exe",
                "C:\\Windows\\AppPatch\\sysmain.sdb",
                "C:\\Windows\\Branding\\ShellBrd\\shellbrd.dll",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\displayswitch.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\displayswitch.lnk",
                "C:\\Windows\\System32\\displayswitch.exe",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Calculator.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Calculator.lnk",
                "C:\\Windows\\System32\\calc.exe",
                "C:\\Windows\\System32\\en-US\\calc.exe.mui",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Sticky Notes.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Sticky Notes.lnk",
                "C:\\Windows\\System32\\StikyNot.exe",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Snipping Tool.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Snipping Tool.lnk",
                "C:\\Windows\\System32\\SnippingTool.exe",
                "C:\\Windows\\System32\\snippingtool.exe",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Paint.lnk",
```

```
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Paint.lnk",
                "C:\\Windows\\System32\\mspaint.exe",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\XPS
Viewer.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\XPS
Viewer.lnk",
                "C:\\Windows\\System32\\xpsrchvw.exe",
                "C:\\Windows\\System32\\en-US\\imageres.dll.mui",
                "C:\\Windows\\System32\\en-US\\xpsrchvw.exe.mui",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Windows Fax and Scan.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Windows Fax and Scan.lnk",
                "C:\\Windows\\System32\\WFS.exe",
                "C:\\Windows\\System32\\WFSR.dll",
                "C:\\Windows\\System32\\en-US\\wfsr.dll.mui",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Remote Desktop Connection.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start
Menu\\Programs\\Accessories\\Remote Desktop Connection.lnk",
                "C:\\Windows\\System32\\mstsc.exe",
                "C:\\Windows\\System32\\en-US\\mstsc.exe.mui",
                "C:\\Windows\\System32\\DeviceCenter.dll",
                "C:\\Windows\\System32\\en-US\\DeviceCenter.dll.mui",
                "%USERPROFILE%\\Desktop\\brpUbjDbMoajfhMqG.ppt",
                "%USERPROFILE%
\\AppData\\Roaming\\Microsoft\\Windows\\Libraries\\desktop.ini",
                "%USERPROFILE%\\Desktop\\brpUbjDbMoajfhMqG.ppt",
                "%USERPROFILE%\\Desktop\\lpcCtTSICymz.ppt",
                "%USERPROFILE%\\Desktop\\lpcCtTSICymz.ppt",
                "%USERPROFILE%\\Desktop\\VYynFmUIpZL.doc",
                "%USERPROFILE%\\Desktop\\VYynFmUIpZL.doc",
                "C:\\Program Files\\Windows NT\\Accessories\\wordpad.exe",
                "C:\\Program Files\\Windows NT\\Accessories\\en-US\\WORDPAD.EXE.
mui",
                "C:\\Windows\\System32\\tzres.dll",
                "C:\\Windows\\System32\\en-US\\tzres.dll.mui",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Media
Center.lnk",
                "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Media
Center.lnk",
                "C:\\Windows\\ehome\\ehshell.exe",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\WER\\ERC\\statecache.lock",
                "%USERPROFILE%
\\AppData\\Local\\Microsoft\\Windows\\WER\\ReportArchive",
                "C:\\ProgramData\\Microsoft\\Windows\\WER\\ReportArchive",
                "%USERPROFILE%\\Desktop\\VYynFmUIpZL.doc",
                "%USERPROFILE%\\Desktop\\XIpLgYiMquIrwvQhRzR.txt",
                "%USERPROFILE%\\Desktop\\UggJFkqdigUrqJZ.docx",
                "%USERPROFILE%\\Desktop\\rUGsdBtIksBG.docm",
                "%USERPROFILE%\\Desktop\\pJZwUGnPDUYzkrE.rtf",
                "%USERPROFILE%\\Desktop\\lpcCtTSICymz.ppt",
                "%USERPROFILE%\\Desktop\\LavcTBslYpi.rtf",
                "%USERPROFILE%\\Desktop\\DIWlsoASJMPKh.docx",
                "%USERPROFILE%\\Desktop\\brpUbjDbMoajfhMqG.ppt",
                "C:\\Windows\\win.ini"
              ]
            },
            "process_activity": [],
            "service_activity": {
              "services_opened": [
                {
                  "service_name": "wscsvc",
                  "argument": null
                }
              ]
            },
            "registry_activity": {
              "set_values": [
                {
                  "key": "HKEY_CURRENT_USER\\Local
Settings\\MuiCache\\2\\52C64B7E\\LanguageList",
                  "value_name": "en-USu0000enu0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExt
s\\.il\\OpenWithList\\MRUList",
                  "value_name": "a",
                  "value_set_data": null
                },
```

```
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UserAss
ist\\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\\Count\\{Q65231O0-O2S1-4857-N4PR-
N8R7P6RN7Q27}\\pzq.rkr",
                  "value_name":
"u0000u0000u0000u0000u0000'u0000u0000u00005u0000u0000u0000u0014rLu0000u0000u0000u0080u00
bfu0000u0000u0080u00bfu0000u0000u0080u00bfu0000u0000u0080u00bfu0000u0000u0080u00bfu
0000u0000u0080u00bfu0000u0000u0080u00bfu0000u0000u0080u00bfu0000u0000u0080u00bfu000
0u0000u0080u00bfu00ffu00ffu00ffu00ffu00c0u00d8u008du00edu00a0u00eeu00d2u0001u0000u0
000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UserAss
ist\\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\\Count\\HRZR_PGYFRFFVBA",
                  "value_name":
"u0000u0000u0000u0000u009cu0000u0000u0000u0010u0001u0000u0000>u0000u00c2u0000'u0000
u0000u00005u0000u0000u0000u0014rLu0000
{u0000Du00006u00005u00002u00003u00001u0000Bu00000u0000-
u0000Bu00002u0000Fu00001u0000-u00004u00008u00005u00007u0000-
u0000Au00004u0000Cu0000Eu0000-
u0000Au00008u0000Eu00007u0000Cu00006u0000Eu0000Au00007u0000Du00002u00007u0000}
u0000\\u0000cu0000mu0000du0000.
u0000eu0000x30xu0000eu0000u0000u0000u00feu0001u00a8u00f0u00feu0001Xu0012u00beu0004u
00ed'u00dfuu0000u0000u0007u0000fu0000u0001u0001Vu0001u0000u0000u0000u0000u0000u0000
*u00b9u0004u0000eu0007u0000u001cfu0007u0000ru0000u00a8u0004Vu0001u0000u0000u00d4u00
00u0000u0000u0084u00e7u00feu0001u0010hu0007u0000u00bcu00fau00feu0001u009bu0002u0000
u0000u00c2wu0019u0000u0000u0000u0000u0000`ru00b4u0002u0000eu0007u0000u00e4fu0007u00
00u00f0u0082u00b4u0002u00b0}
u0007u0000Mu00d7Gwu00b4u00e7u00feu0001u00feu00ffu00ffu00ffu00bcu00fau00feu0001Mu00d
7Gwu00c2wu0019u0000u00feu00ffu00ffu00ffu00ae\"KwI!
Kwu009bu0002u0000u0000u0098u0085u00b4u0002|u0012u00beu0004u0000u00b3u00bdu0",
                  "value_set_data": null
                },
                {
                  "key": "HKEY_CURRENT_USER\\Local
Settings\\MuiCache\\2\\52C64B7E\\@C:\\Program Files\\Windows
NT\\Accessories\\WORDPAD.EXE,-190",
                  "value_name": "Rich Text Document",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.101\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0001u0000
u0000u0000u00a0u0000u0000u0000u0000u0000u0000u0000u0000u001cu00f1u0088u00fcu008eYu00d3u0
001u0000u0000u0000u0000{u0000Eu00008u00004u00003u00003u0000Bu00007u00002u0000-
u00005u00008u00004u00002u0000-u00004u0000du00004u00003u0000-
u00008u00006u00004u00005u0000-
u0000Bu0000Cu00002u0000Cu00003u00005u00009u00006u00000u00008u00003u00007u0000}
u0000.
u0000nu0000ou0000tu0000iu0000fu0000iu0000cu0000au0000tu0000iu0000ou0000nu0000.
u00001u00000u00001u0000.u00002u0000-
u00007u00003u00009u00009u00007u00003u00004u0000u0000u0000u0000u0000u0000u0000u0000u
0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.103\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0001u0000
u0000u0000u00a0u0000u0000u0000u0000u0000u0000u0000u0000vSu008bu00fcu008eYu00d3u0001u0000
u0000u0000u0000{u0000Eu00008u00004u00003u00003u0000Bu00007u00002u0000-
u00005u00008u00004u00002u0000-u00004u0000du00004u00003u0000-
u00008u00006u00004u00005u0000-
u0000Bu0000Cu00002u0000Cu00003u00005u00009u00006u00000u00008u00003u00007u0000}
u0000.
u0000nu0000ou0000tu0000iu0000fu0000iu0000cu0000au0000tu0000iu0000ou0000nu0000.
u00001u00000u00003u0000.u00002u0000-
u00007u00003u00009u00009u00007u00005u00000u0000u0000u0000u0000u0000u0000u0000u0000u
0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.100\\CheckSetting",
                  "value_name":
```

```
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0001u0000
u0000u0000u00a0u0000u0000u0000u0000u0000u0000u0000u0000vSu008bu00fcu008eYu00d3u0001u0000
u0000u0000u0000{u0000Eu00008u00004u00003u00003u0000Bu00007u00002u0000-
u00005u00008u00004u00002u0000-u00004u0000du00004u00003u0000-
u00008u00006u00004u00005u0000-
u0000Bu0000Cu00002u0000Cu00003u00005u00009u00006u00000u00008u00003u00007u0000}
u0000.
u0000nu0000ou0000tu0000iu0000fu0000iu0000cu0000au0000tu0000iu0000ou0000nu0000.
u00001u00000u00000u0000.u00001u0000-
u00007u00003u00009u00009u00007u00005u00000u0000u0000u0000u0000u0000u0000u0000u0000u0000u
0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.102\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0001u0000
u0000u0000u00a0u0000u0000u0000u0000u0000u0000u0000u0000vSu008bu00fcu008eYu00d3u0001u0000
u0000u0000u0000{u0000Eu00008u00004u00003u00003u0000Bu00007u00002u0000-
u00005u00008u00004u00002u0000-u00004u0000du00004u00003u0000-
u00008u00006u00004u00005u0000-
u0000Bu0000Cu00002u0000Cu00003u00005u00009u00006u00000u00008u00003u00007u0000}
u0000.
u0000nu0000ou0000tu0000iu0000fu0000iu0000cu0000au0000tu0000iu0000ou0000nu0000.
u00001u00000u00002u0000.u00003u0000-
u00007u00003u00009u00009u00007u00005u00000u0000u0000u0000u0000u0000u0000u0000u0000u0000u
0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0000u0000u0000
u0000u0000u0001u0000u0000u0000pu0000eu0000u0000u0000u0000:",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0000u0000u0000
u0000u0000u0001u0000u0000u0000pu0000eu0000u0000u0000u0000:",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0000u0000u0000
u0000u0000u0001u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0001u0000
u0000u0000u0080u0000u0000u0000cu0000ku0000u00cau00bfu00c0#u0013u00ebu00d2u0001u0000
u0000u0000u0000{u00000u00001u00009u00007u00009u0000cu00006u0000au0000-
u00004u00002u0000fu0000au0000-u00004u00001u00004u0000cu0000-
u0000bu00008u0000au0000au0000-
u0000eu0000eu0000eu00002u0000cu00008u00002u00000u00002u00000u00001u00008u0000}
u0000.
u0000nu0000ou0000tu0000iu0000fu0000iu0000cu0000au0000tu0000iu0000ou0000nu0000.
u00000u0000u0000u0000yu0000-u0000mu0000su0000u0000u0000u0000",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{945a8954-c147-4acd-923f-40c45405a658}.check.42\\CheckSetting",
                  "value_name":
"#u0000Au0000Cu0000Bu0000lu0000ou0000bu0000u0000u0000u0000u0000u0000u0000u0000u0000u0000
u0000u0000u0001u0000u0000u0000eu0000du0000u0000u0000u0000u0000u0000",
                  "value_set_data": null
                }
              ],
```

```
              "created_keys": [

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExt
s\\.il\\OpenWithList",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.106",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.101",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.103",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.100",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.102",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{E8433B72-5842-4d43-8645-BC2C35960837}.check.104",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.100",
                "HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\Windows Error
Reporting",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{852FB1F8-5CC6-4567-9C0E-7C330F8807C2}.check.101",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Providers\\EventLog\\{01979c6a-42fa-414c-b8aa-eee2c8202018}",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Providers\\EventLog\\{945a8954-c147-4acd-923f-40c45405a658}",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{945a8954-c147-4acd-923f-40c45405a658}.check.42",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Providers\\EventLog\\{DAB69A6A-4D2A-4D44-94BF-E0091898C881}",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{DAB69A6A-4D2A-4D44-94BF-E0091898C881}.check.100",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Providers\\EventLog\\{11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78}",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78}.check.101",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Providers\\EventLog\\{A5268B8E-7DB5-465b-BAB7-BDCDA39A394A}",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Action
Center\\Checks\\{A5268B8E-7DB5-465b-BAB7-BDCDA39A394A}.check.100"
              ]
            },
            "mutex_activity": {
              "created_mutex": [
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_idx.db!rwWriterMutex",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_32.db!dfMaintainer",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_96.db!dfMaintainer",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_256.db!dfMaintainer",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_1024.db!dfMaintainer",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_sr.db!dfMaintainer",
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_idx.db!ThumbnailCacheInit",
```

```
                "Global\\C::Users:Patrick:AppData:Local:Microsoft:Windows:Explorer:
thumbcache_idx.db!rwReaderRefs"
              ],
              "used_mutex": [
                "DefaultTabtip-MainUI",
                "CicLoadWinStaWinSta0",
                "Local\\MSCTF.CtfMonitorInstMutexDefault1"
              ]
            },
            "window_activity": []
          },
          {
            "process": "C:\\Windows\\ehome\\ehshell.exe",
            "file_activity": {
              "deleted_files": [
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Blocks.mem",
                "c:\\programdata\\microsoft\\eHome\\Counter.mem",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Root.mem",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Events.mem"
              ],
              "read_files": [
                "C:\\Windows\\Globalization\\Sorting\\sortdefault.nls",
                "C:\\Windows\\ehome\\ehshell.exe.config",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727
\\CONFIG\\machine.config",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727
\\CONFIG\\security.config",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727
\\CONFIG\\security.config.cch",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727
\\CONFIG\\enterprisesec.config",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727
\\CONFIG\\enterprisesec.config.cch",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\CLR Security
Config\\v2.0.50727.312\\security.config",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\CLR Security
Config\\v2.0.50727.312\\security.config.cch",
                "C:\\Windows\\assembly\\NativeImages_v2.0.50727_32\\indexbc.dat",
                "C:\\Windows\\System32\\l_intl.nls",
                "C:\\Windows\\assembly\\GAC_32\\mscorlib\\2.0.0.0
__b77a5c561934e089\\sorttbls.nlp",
                "C:\\Windows\\assembly\\GAC_32\\mscorlib\\2.0.0.0
__b77a5c561934e089\\sortkey.nlp",
                "C:\\Windows\\ehome\\ehshell.exe",
                "C:\\Windows\\assembly\\GAC_32\\mcstoredb\\6.1.0.0
__31bf3856ad364e35\\mcstoredb.dll",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Blocks.mem",
                "c:\\programdata\\microsoft\\eHome\\Counter.mem",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Root.mem",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0.db",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0.db",
                "c:\\programdata\\microsoft\\eHome\\mcepg2-0\\Events.mem",
                "C:\\Windows\\ehome\\ehepgres.dll",
                "%USERPROFILE%\\AppData\\Roaming\\Microsoft\\eHome\\ehshell.
config",
                "C:\\Windows\\assembly\\GAC_32\\BDATunePIA\\6.1.0.0
__31bf3856ad364e35\\BDATunePIA.dll",
                "C:\\Windows\\System32\\kstvtune.ax",
                "C:\\Windows\\assembly\\GAC_MSIL\\Microsoft.MediaCenter.UI\\6.1.0.0
__31bf3856ad364e35\\Microsoft.MediaCenter.UI.dll",
                "C:\\Windows\\ehome\\ehshell.dll",
                "C:\\Windows\\assembly\\GAC_MSIL\\ehshell\\6.1.0.0
__31bf3856ad364e35\\ehshell.dll",
                "C:\\Windows\\ehome\\Microsoft.MediaCenter.Shell.dll",
                "C:\\Windows\\assembly\\GAC_MSIL\\Microsoft.MediaCenter.Shell\\6.
1.0.0__31bf3856ad364e35\\Microsoft.MediaCenter.Shell.dll",
                "C:\\Windows\\Microsoft.NET\\Framework\\v2.0.50727\\mscorrc.dll",
                "C:\\ProgramData\\Microsoft\\eHome\\ehshell.config",
                "C:\\ProgramData\\Microsoft\\eHome\\logs\\FirstRun.log",
                "C:\\Windows\\ehome\\mcstore.dll",
                "C:\\Windows\\assembly\\GAC_MSIL\\mcstore\\6.1.0.0
__31bf3856ad364e35\\mcstore.dll",
                "C:\\Windows\\ehome\\mcepg.dll",
                "C:\\Windows\\assembly\\GAC_MSIL\\mcepg\\6.1.0.0
__31bf3856ad364e35\\mcepg.dll",
                "C:\\Windows\\System32\\spool\\drivers\\color\\sRGB Color Space
Profile.icm",
                "C:\\Windows\\assembly\\GAC_32\\Microsoft.MediaCenter.Interop\\6.
1.0.0__31bf3856ad364e35\\Microsoft.MediaCenter.Interop.dll",
                "C:\\Windows\\assembly\\GAC_32\\Mcx2Dvcs\\6.1.0.0
__31bf3856ad364e35\\Mcx2Dvcs.dll",
                "C:\\ProgramData\\Microsoft\\eHome\\mcepg2-0.db",
                "C:\\Windows\\win.ini",
                "C:\\Windows\\System32\\OEMINFO.INI"
```

```
            ]
          },
          "process_activity": [],
          "service_activity": {
            "services_opened": [
              {
                "service_name": "AudioSrv",
                "argument": "SERVICE_QUERY_STATUS"
              },
              {
                "service_name": "AudioSrv",
                "argument": "SERVICE_QUERY_CONFIG|SERVICE_QUERY_STATUS"
              }
            ]
          },
          "registry_activity": {
            "created_keys": [

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\MediaPlayer\\Preferences\\",

"HKEY_CURRENT_USER\\Software\\Microsoft\\MediaPlayer\\Preferences\\",

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Fusion\\GACChangeNotification\\Default",

"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Capabilities",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings",

"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings",

"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig",

"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings",

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\PvrRecoveryTask",

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\ObjectStoreRecoveryTask",

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\SqlLiteRecoveryTask",

"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\OOBERecoveryTask",
              "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Cryptography\\RNG"
            ],
            "set_values": [
              {
                "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\EPG\\clientid",
                "value_name": "a1778d1a5c6247248c6c9d735df88f56",
                "value_set_data": null
              },
              {
                "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\monitor",
                "value_name": "",
                "value_set_data": null
              },
              {
                "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\top",
                "value_name": "0",
                "value_set_data": null
              },
              {
                "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\left",
                "value_name": "0",
                "value_set_data": null
              },
              {
                "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\MCE.PerUserSettings\\width",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\height",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\showCmd",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\marginLeft",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\marginTop",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\marginRight",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\marginBottom",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\marginSaved",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableStartupAnimation",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableStartupSound",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableBgAnimations",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableAnimations",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\MCE.PerUserSettings\\enableUnderline",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableNTSC",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\enableAlwaysOnTop",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\skipDefaultShellCheck",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\useDefaultOverscanMargins",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\soundEffectsEnabled",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\soundEffectsUpgraded",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\startGrovelOnLaunch",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\optimizeFor",
                  "value_name": "ComputerMonitor",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\highContrastMode",
                  "value_name": "Off",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\fAllowRatingShortcuts",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\fGadgetAddPrompted",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\MCE.PerUserSettings\\showOskOnKeyboardEnter",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SetupUserLibraryId",
                  "value_name": "<<NULL>>",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\ExtenderSetupUserName",
                  "value_name": "<<NULL>>",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmFrunWelcomeDialogOption",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmFrunOptionalSettings",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmSettingsDisplayType",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmFrunDisplayConnectionType",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmVisualSettings",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmSpeakerSettingsConfig",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmSpeakerSettingsType",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmSetingsStartupAndWindowsBehavior",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmSettingsDisplayWidth",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\MCE.PerUserSettings\\autoSlideshowOption",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmHasBattery",
                  "value_name": "Uninitialized",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\Version",
                  "value_name": "65537",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iVideoSource",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iConfigured",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iAtscVideoSource",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iBroadcastStandard",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\fHasSTB",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\fHasDVB",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\fAtscOnly",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\fAllowDvbsMHEG",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\fPbdaConfigured",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\TVConfig\\iSqmStbFinishedSetup",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbCount",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbLearningUsed1",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbSelectedFromList1",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbType",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbCodeSet1",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbUseEnter1",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iSqmStbTwoIdenticalBoxes",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iUpgradeStatus",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\iUpgradeDialogChoice",
                  "value_name": "2",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\TVConfig\\Version",
                  "value_name": "65537",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\CurrentModule",
                  "value_name": "4294967295",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\FirstRunRegSettings\\CurrentSequence",
                  "value_name": "",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\CalledFrom",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\RunWizardAgain",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\strAlreadyDoneChoices",
                  "value_name": "",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\Version",
                  "value_name": "65537",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\fAgreeTOS",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\fPrivacyLevel",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\fDisableAutoFavorites",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\strLocation",
                  "value_name": "<<NULL>>",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\strCountryCode",
                  "value_name": "<<NULL>>",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\strAgreedTOSVersion",
                  "value_name": "",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\ProgramGuide\\fUsageTracking",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\ProgramGuide\\Version",
                  "value_name": "65537",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\CurrentModule",
                  "value_name": "0",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\CurrentSequence",
                  "value_name": "1|4|2|13|8|9|18",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\CalledFrom",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\FirstRunRegSettings\\RunWizardAgain",
                  "value_name": "1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\PvrRecoveryTask\\LastActionCheck",
                  "value_name": "11/9/2017 11:14:18 AM",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\ObjectStoreRecoveryTask\\LastActionCheck",
                  "value_name": "11/9/2017 11:14:18 AM",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\SqlLiteRecoveryTask\\LastActionCheck",
                  "value_name": "11/9/2017 11:14:18 AM",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\RecoveryTasks\\OOBERecoveryTask\\LastActionCheck",
                  "value_name": "11/9/2017 11:14:18 AM",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\monitor",
                  "value_name": "\\\\.\\DISPLAY1",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\top",
                  "value_name": "25",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\width",
                  "value_name": "800",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
```

```
Center\\Settings\\MCE.PerUserSettings\\height",
                  "value_name": "449",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Settings\\MCE.PerUserSettings\\SqmHasBattery",
                  "value_name": "False",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\MediaPlayer\\Preferences\\TrackFoldersDire
ctories7",
                  "value_name": "C:\\Users\\$USER$\\Recorded TV\\",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_CURRENT_USER\\Software\\Microsoft\\MediaPlayer\\Preferences\\TrackFoldersDire
ctories",
                  "value_name": "8",
                  "value_set_data": null
                },
                {
                  "key":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Media
Center\\Service\\EPG\\MediaCenterLastUsed",
                  "value_name": "131547284777031250",
                  "value_set_data": null
                }
              ]
            },
            "mutex_activity": {
              "created_mutex": [
                "eHomeNameMutex",
                "Local\\__DDrawExclMode__",
                "Local\\__DDrawCheckExclMode__",
                "DirectSound Administrator shared thread array (lock)",
                "RasPbFile",
                "Global\\MCStoreOpen_b4cae1f9a3aead62bebb934ca33cadb730c8d3ed",
                "Global\\MCStoreSyncMem_5ea381292eeb3ed3e61dc84a3dbd4d7f59767eca",
                "Global\\MCStoreSyncMem_7715dc857070a1523dea43f32f1fe67c1ce58e0b",
                "Global\\MCStoreSyncMem_71bdfe29063ac557a4e7b3205ed180408457fcd4",
                "Global\\eHome_DbMutex_1",
                "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-0.db",
                "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-0.db:x",
                "Global\\__?_c:_programdata_microsoft_ehome_mcepg2-0.db:splk:1944",
                "Global\\MCStoreSyncMem_02004a9f865399b5c2a02973d5e53544ed4ce2ea",
                "Global\\eHome_DbRWMutex_1",
                "Global\\eHome_DbMutex_2",
                "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:sqlce_se_lck:1",

"Global\\MCStoreCreateTable_a1d78cdcc411921ce3b07770aa2a0e0745789b11",
                "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:sqlce_se_lck:2",

"Global\\MCStoreAddStoredType_a1d78cdcc411921ce3b07770aa2a0e0745789b11",
                "Global\\eHome_DbMutex_3",
                "Global\\eHome_DbMutex_4",
                "Global\\eHome_DbMutex_5",
                "Global\\MediaCenter.
MCUpdate_7000000000026_a1d78cdcc411921ce3b07770aa2a0e0745789b11",
                "Global\\{48a4b2ff-ebd1-4288-8215-f3c0ade89db7}:sqlce_se_lck:3",
                "Local\\MICROSOFT_WMDM_MUTEX",
                "Global\\ReinitMCUpdate_a1d78cdcc411921ce3b07770aa2a0e0745789b11",
                "Global\\eHome_DbRWMutex_2",
                "Global\\eHome_DbMutex_6",
                "Global\\eHome_DbMutex_7",
                "Global\\eHome_DbRWMutex_3",
                "Global\\eHome_DbMutex_8"
              ],
              "used_mutex": [
                "Global\\CLR_CASOFF_MUTEX"
              ]
            },
            "window_activity": []
          }
        ],
        "dropped_files": [],
        "network": {
          "dns": [
            {
              "dst_ip": "10.3.10.11",
```

```
              "dst_port": "53",
              "protocol": "udp",
              "query": "time.windows.com",
              "query_type": "1",
              "r_code": null,
              "answers": null,
              "rejected": "0",
              "response_geo_ip": null
            },
            {
              "dst_ip": "10.3.10.11",
              "dst_port": "53",
              "protocol": "udp",
              "query": "teredo.ipv6.microsoft.com",
              "query_type": "1",
              "r_code": null,
              "answers": null,
              "rejected": "0",
              "response_geo_ip": null
            },
            {
              "dst_ip": "10.3.10.11",
              "dst_port": "53",
              "protocol": "udp",
              "query": "watson.microsoft.com",
              "query_type": "1",
              "r_code": null,
              "answers": null,
              "rejected": "0",
              "response_geo_ip": null
            },
            {
              "dst_ip": "10.3.10.11",
              "dst_port": "53",
              "protocol": "udp",
              "query": "dns.msftncsi.com",
              "query_type": "1",
              "r_code": null,
              "answers": null,
              "rejected": "0",
              "response_geo_ip": null
            }
          ],
          "http": [],
          "ssl": [],
          "conn": []
        }
      }
    }
  ]
}
```