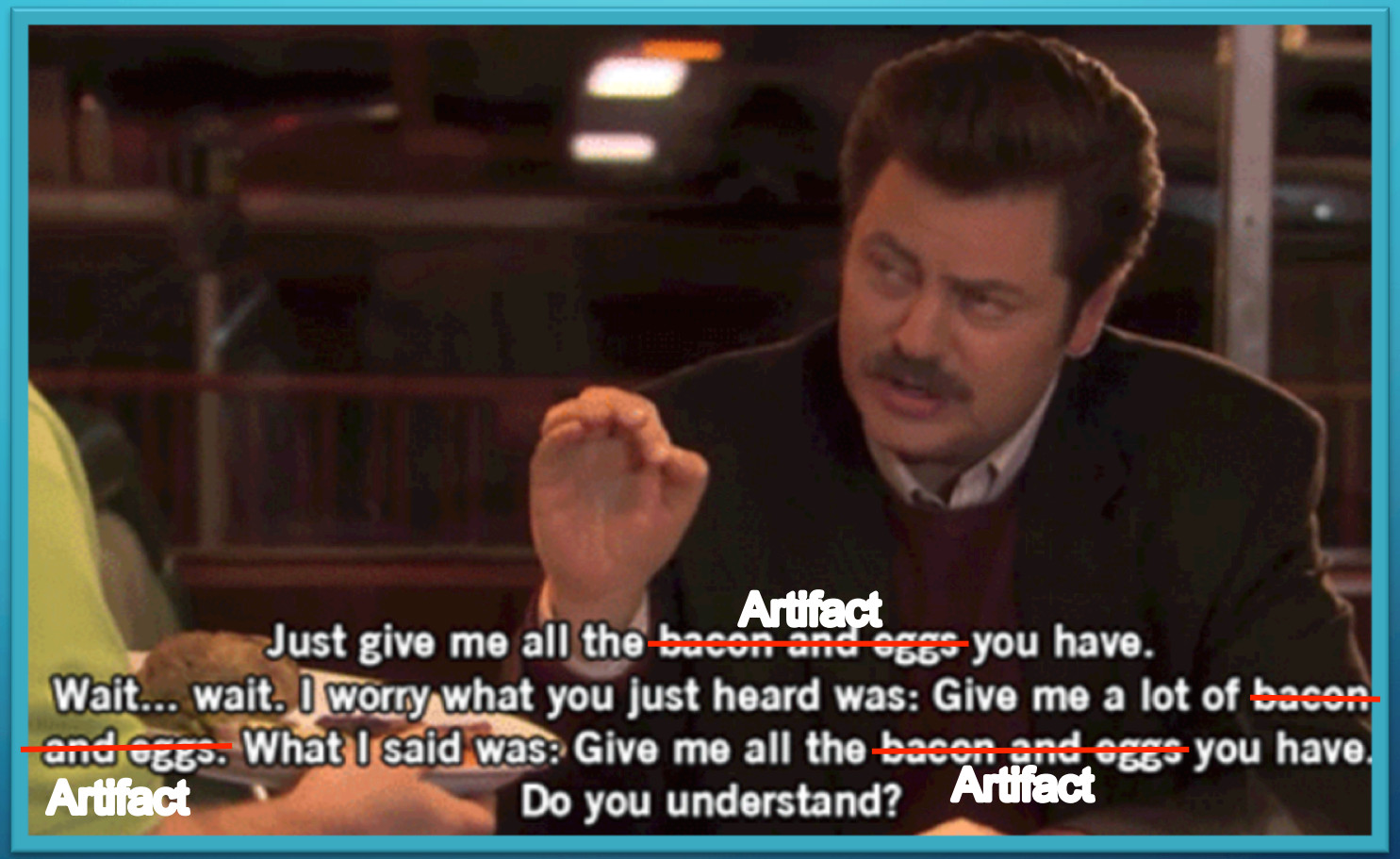
SHOW ME ALL OF YOUR ARTIFACT!

USING SQLITE JSON OBJECTS TO STORE ALL OF THE ARTIFACT


Artifact
Just give me all the ~~bacon and eggs~~ you have.
Wait... wait. I worry what you just heard was: Give me a lot of ~~bacon~~
~~and eggs.~~ What I said was: Give me all the ~~bacon and eggs~~ you have.
Artifact
Artifact
Do you understand?

WHY HAVE DIFFERENT TYPES OF OUTPUT?

- Output for Analysis
- Output for People
  - Sometimes the output for people takes valuable information away from the analyst

CORRELATION POINTS

- Can’t correlate artifacts if the correlation point is not present
- Example
  - IDLists in linkfiles can correlate to Shellbags for external device access.

THAT'S A LOT OF ARTIFACTS!

LogFile

Shell Bag

MFT

Prefetch

USN

Link File

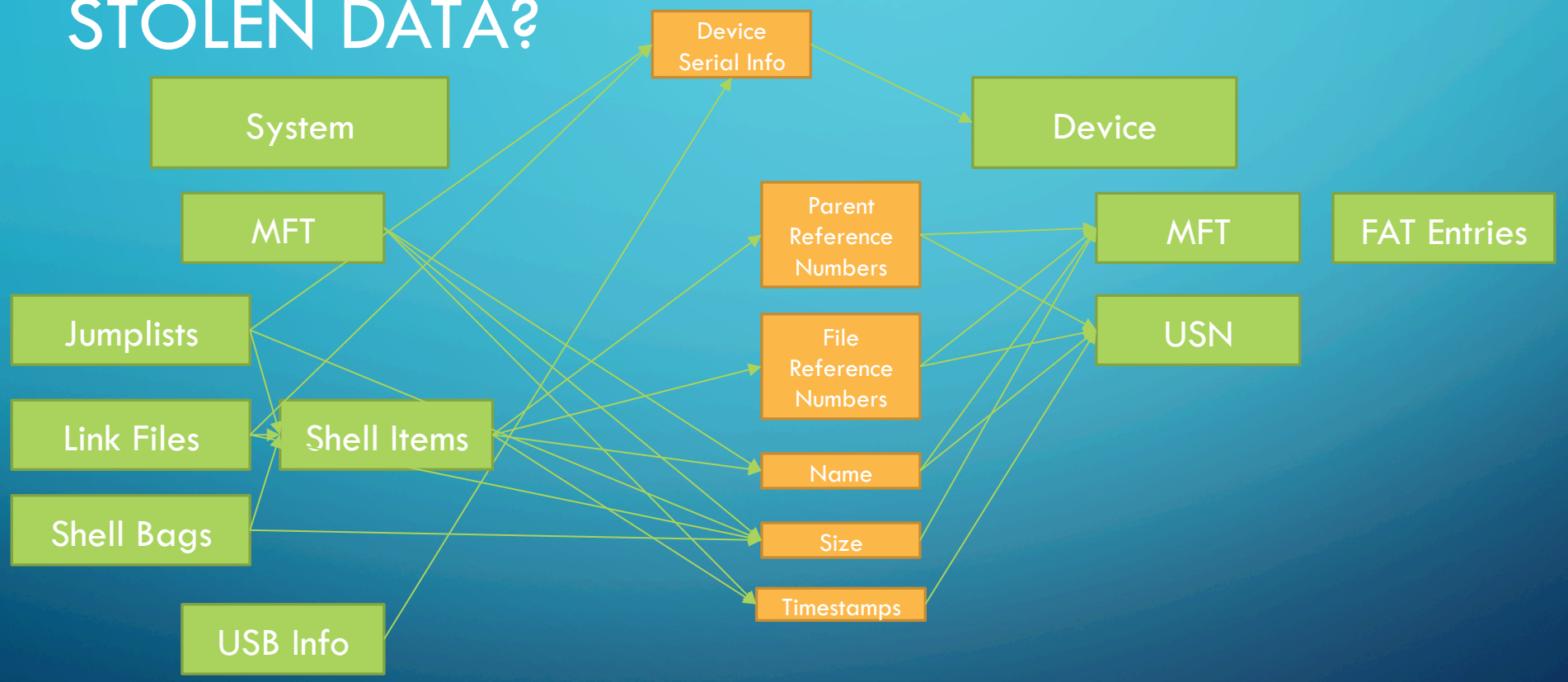
Jump List

Shim Cache

Event Logs

THAT'S A LOT OF CORRELATION!

STOLEN DATA?


System
MFT
Jumplists
Link Files
Shell Items
Shell Bags
USB Info
Device Serial Info
Parent Reference Numbers
File Reference Numbers
Name
Size
Timestamps
Device
MFT
USN
FAT Entries

FLAT OUTPUT

- Easy for review
- Easy to stick into excel, make pretty, and send off to client
- Easy to sort and filter

example.gc_lnk_report.tsv

```
DriveType    DriveSerialNumber    VolumeLabel LocalPath    NetworkPath RelativePath    AppIdCode    AppIdName    BaseName    FileExt DLE_EntryNum    DLE_BirthDroidVolId DLE_BirthDroidFile
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Windows\System32\CanonIJ Uninstaller Information\{1199FAD5-9546-44f3-81CF-FFDB8040B7BF}_Canon_MX870_series\DelDrv64.exe    ..\..\..\..\..
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Program Files (x86)\Mozilla Firefox\firefox.exe    ..\..\..\..\..\Program Files (x86)\Mozilla Firefox\firefox.exe    firefox.exe ex
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Program Files (x86)\Mozilla Firefox\firefox.exe    ..\..\..\Program Files (x86)\Mozilla Firefox\firefox.exe    firefox.exe exe
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Users\Donald\SkyDrive\Pictures\Camera Roll    ..\..\..\..\..\SkyDrive\Pictures\Camera Roll    Camera Roll
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Program Files (x86)\Google\Chrome\Application\chrome.exe    ..\..\..\Program Files (x86)\Google\Chrome\Application\chrome.exe    ch
DRIVE_FIXED;    7e58-aab0    Windows8_OS C:\Program Files (x86)\Google\Chrome\Application\chrome.exe    ..\..\..\..\..\..\..\Program Files (x86)\Google\Chrome\Application\chrome.exe
```

	A	B	C	D	I	J	S	T
1	DriveType	DriveSerialNumb	VolumeLabel	LocalPath	BaseName	FileExt	CreationDateTime	ModificationDate
70	DRIVE_REMOVABLE;	39c7-1beb	USB	F:\Business Plan for a Startup Business_0.doc	Business Plan for a Startup Business_	doc	10/21/2013 18:53:01	10/13/2013 12:45:02
71	DRIVE_REMOVABLE;	440f-17ad	PHOTOS BACK	E:\WP_20130803_001.jpg	WP_20130803_001.jpg	jpg	10/17/2013 19:29:04	8/3/2013 19:28:58
73	DRIVE_REMOVABLE;	440f-17ad	PHOTOS BACK	E:\From Donald's Windows Phone\Saved pictures\imagesCAL5YVMT.jpg	imagesCAL5YVMT.jpg	jpg	10/17/2013 19:29:10	9/2/2013 20:02:28
74	DRIVE_REMOVABLE;	440f-17ad	PHOTOS BACK	E:\From Donald's Windows Phone\Saved pictures	Saved pictures		10/17/2013 19:29:10	10/12/2013 17:35:30
346	DRIVE_REMOVABLE;	39c7-1beb	USB	F:\			1/1/1980 4:00:00	1/1/1980 4:00:00
454	DRIVE_REMOVABLE;	39c7-1beb	USB	F:\			1/1/1980 4:00:00	1/1/1980 4:00:00
456	DRIVE_REMOVABLE;	39c7-1beb	USB	F:\Templates\business_plan1.doc	business_plan1.doc	doc	10/21/2013 20:16:25	10/21/2013 19:47:30

NESTED OUTPUT

- Contains data that does not have room in flat output
  - Can lead to more correlation points
- Can show the proper structure of an artifact
- Can contain unstructured data
- Common formats – JSON, XML, YAML

example.gc_lnk_report.json


```
1  {
2      "lnk_files": [
3          {
4              "VolumeLabel": "Windows8_OS",
5              "BaseName": "DelDrv64.exe",
6              "WorkingDir": null,
7              "LocalPath": "C:\\Windows\\System32\\CanonIJ Uninstaller Infor
8              "ModificationDateTime": "09/10/2009 13:12:10.000000",
9              "CmdArgs": "/U:{1199FAD5-9546-44f3-81CF-FFDB8040B7BF}_Canon_MX
10             "Source": "f:\\SANS408\\Donald_Blake_Evidence\\C-Drive\\Extrac
11             "Flags": "Archive;",
12             "DriveType": "DRIVE_FIXED;",
13             "AccessDateTime": "08/31/2013 03:48:12.113105",
14             "DriveSerialNumber": "7e58-aab0",
15             "AppIdCode": null,
16             "LnkTrgData": {
17                 "DistinctTypesHex": "0x32L;0x2fL;0x1fL;0x31L",
18                 "ParentSeqNum": 5,
19                 "ParentRefStr": "101676-5",
20                 "FileEntries": [
21                     {
22                         "ShellFolderId": null,
23                         "ShellItemTypeHex": "0x31L",
24                         "Identifier": null,
25                         "Name": "Windows",
26                         "Location": null,
27                         "Comments": null,
28                         "ModificationTime": "08/12/2013 03:07:06.000000",
29                         "ShellItemTypeStr": "file_entry",
30                         "ExtentionBlockCount": 1,
31                         "Description": null,
```


JSON file

JSON OBJECTS IN SQLITE

- You get all the artifact
- You can do better filtering
- You decide how you output it

WINDOWS EVENT STRUCTURE - XML


```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
 <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}"/>
  <EventID>4648</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2013-09-20T20:32:40.903544000Z"/>
  <EventRecordID>1206752</EventRecordID>
  <Correlation/>
  <Execution ProcessID="732" ThreadID="9668"/>
  <Channel>Security</Channel>
  <Computer>Bifrost</Computer>
  <Security/>
 </System>
 <EventData>
  <Data Name="SubjectUserSid">S-1-5-18</Data>
  <Data Name="SubjectUserName">BIFROST$</Data>
  <Data Name="SubjectDomainName">ASGARD</Data>
  <Data Name="SubjectLogonId">0x00000000000003e7</Data>
  <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TargetUserName">dblake@asgard-venture-capital.com</Data>
  <Data Name="TargetDomainName">MicrosoftAccount</Data>
  <Data Name="TargetLogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TargetServerName">localhost</Data>
  <Data Name="TargetInfo">localhost</Data>
  <Data Name="ProcessId">0x00000000000002a8</Data>
  <Data Name="ProcessName">C:\Windows\System32\winlogon.exe</Data>
  <Data Name="IpAddress">127.0.0.1</Data>
  <Data Name="IpPort">0</Data>
 </EventData>
</Event>
```


*The problem is this data is dynamic and can contain anything.

DYNAMIC EXAMPLES


```
<EventData>
  <Data/>

<Binary>0000080001000000000000001200054000000000000000000000000000000000000000000000000
000E000000000000000</Binary>
 </EventData>
```

```
<EventData>
  <Data>msiexec</Data>
  <Data>3636</Data>
  <Data>Instance: </Data>
  <Data>0</Data>
  <Data>6</Data>
  <Data>02</Data>
  <Data>9200</Data>
  <Data>0000</Data>
</EventData>
```

```
<UserData>
  <AddServiceID xmlns="http://manifests.microsoft.com/win/2004/08/windows/userpnp">
    <ServiceName>WUDFWpdFs</ServiceName>
    <DriverFileName>\SystemRoot\system32\DRIVERS\WUDFRd.sys</DriverFileName>
    <DeviceInstanceID>SWD\WPDBUSENUM\{ABCD082A-3B8E-11E3-BE8D-24FD52566EDE}
#0000000000007E00</DeviceInstanceID>
    <PrimaryService>true</PrimaryService>
    <UpdateService>true</UpdateService>
    <AddServiceStatus>0</AddServiceStatus>
  </AddServiceID>
 </UserData>
```

```
<EventData>
  <Data>Service started successfully.</Data>
</EventData>
```

WINDOWS EVENT STRUCTURE - JSON


```
{

 "EventData": {
   "Data": [{
     "#text": "S-1-5-18",
     "Name": "SubjectUserSid"
   },
   {
     "#text": "BIFROST$",
     "Name": "SubjectUserName"
   },
   {
     "#text": "ASGARD",
     "Name": "SubjectDomainName"
   },
   {
     "#text": "0x00000000000003e7",
     "Name": "SubjectLogonId"
   },
   {
     "#text":
"{00000000-0000-0000-0000-000000000000}",

     "Name": "LogonGuid"
   },
   {
     "#text": "dblake@asgard-venture-capital.com",
     "Name": "TargetUserName"
   },
   {
     "#text": "MicrosoftAccount",
     "Name": "TargetDomainName"
   },
   {
     "#text":
"{00000000-0000-0000-0000-000000000000}",
     "Name": "TargetLogonGuid"
   },
   {

     "#text": "localhost",
     "Name": "TargetServerName"
   },
   {
     "#text": "localhost",
     "Name": "TargetInfo"
   },
   {
     "#text": "0x00000000000002a8",
     "Name": "ProcessId"
   },
   {
     "#text": "C:\\Windows\\System32\\winlogon.exe",
     "Name": "ProcessName"
   },
   {
     "#text": "127.0.0.1",
     "Name": "IpAddress"

   },

   {
     "#text": "0",
     "Name": "IpPort"
   }]
 },
 "xmlns": "http://schemas.microsoft.com/win/2004/08/events/event",
 "System": {
   "EventID": {
     "#text": "4648"
   },
   "Task": {

     "#text": "12544"
   },

   "TimeCreated": {
     "SystemTime":
"2013-09-20T20:32:40.903544000Z"
   },
   "Level": {
     "#text": "0"
   },
   "Correlation": {

   },
   "Version": {
     "#text": "0"
   },
   "Opcode": {
     "#text": "0"
   },
   "EventRecordID": {
     "#text": "1206752"
   },
   "Provider": {
     "Guid": "{54849625-5478-4994-
A5BA-3E3B0328C30D}",
     "Name": "Microsoft-Windows-Security-
Auditing"
   },
   "Keywords": {
     "#text": "0x8020000000000000"
   },
   "Security": {

   },
   "Execution": {
     "ProcessID": "732",
     "ThreadID": "9668"

   },
   "Computer": {
     "#text": "Bifrost"
   },
   "Channel": {

     "#text": "Security"
   }
 }
}
```

LOGON ACTIVITY IN WINDOWS EVENTS

```
SELECT
winevent.written_time AS "Time",
winevent.event_identifier AS "EventID",
winevent.we_description AS "Description",
CASE
  WHEN event_identifier == 4624
    THEN json_extract(we_jrec,'$.EventData.Data[5].#text')
  WHEN event_identifier == 4634
    THEN json_extract(we_jrec,'$.EventData.Data[1].#text')
  WHEN event_identifier == 4648
    THEN json_extract(we_jrec,'$.EventData.Data[5].#text') || ' -> ' ||
    json_extract(we_jrec,'$.EventData.Data[1].#text')
  ELSE '<Not Handled>'
  END AS "LogonID",
winevent.computer_name AS "Computer",
winevent.source_name AS "Channel",
winevent.we_source AS "Source"
FROM "winevent"
WHERE
Channel == 'Microsoft-Windows-Security-Auditing' AND
event_identifier IN (4624,4625,4634,4648)
ORDER BY written_time
```

RESULT

Time	EventID	Description	LogonID	Computer	Channel	Source
2013-10-23 02:56:19.619567	4624	An account was successfully logged on	SYSTEM	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:19.900833	4624	An account was successfully logged on	ANONYMOUS LOGON	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.797819	4648	A logon was attempted using explicit credentials	dblake@asgard-venture-capital.com -> BIFROST$	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.797819	4624	An account was successfully logged on	dblake@asgard-venture-capital.com	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.797819	4624	An account was successfully logged on	dblake@asgard-venture-capital.com	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.844717	4648	A logon was attempted using explicit credentials	dblake@asgard-venture-capital.com -> BIFROST$	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.844717	4624	An account was successfully logged on	dblake@asgard-venture-capital.com	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.844717	4624	An account was successfully logged on	dblake@asgard-venture-capital.com	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.844717	4634	An account was logged off	Donald	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:24.844717	4634	An account was logged off	Donald	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:26.063514	4624	An account was successfully logged on	SYSTEM	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:56:46.536368	4624	An account was successfully logged on	SYSTEM	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx
2013-10-23 02:59:21.819795	4624	An account was successfully logged on	ANONYMOUS LOGON	Bifrost	Microsoft-Windows-Security-Auditing	..\testfiles\sans408\Security.evtx

DEMO

- SQLite Templates for Windows Events with EventMonkey
- Templates and the tool can be found here: https://github.com/devgc/EventMonkey

LNK FILE STRUCTURE - JSON


```
{
  "VolumeLabel": "USB",
  "BaseName": "business_plan1.doc",
  "WorkingDir": null,
  "LocalPath": "F:\\Templates\\business_plan1.doc",
  "ModificationDateTime": "10/21/2013
19:47:30.000000",
  "CmdArgs": null,
  "Source": "f:\\SANS408\\Donald_Blake_Evidence\\C-
Drive\\Extracts\\SANS408\\p1-sys\\link-files\
\48409.Donald.business_plan1.LNK",
  "Flags": "Archive;",
  "DriveType": "DRIVE_REMOVABLE;",
  "AccessDateTime": "10/21/2013 04:00:00.000000",
  "DriveSerialNumber": "39c7-1beb",
  "AppIdCode": null,
  "LnkTrgData": {
    "DistinctTypesHex": "0x32L;0x2fL;0x1fL;0x31L",
    "ParentSeqNum": 0,

    "ParentRefStr": "253312-0",
    "FileEntries": [

      {
        "ShellFolderId": null,
        "ShellItemTypeHex": "0x31L",
        "Identifier": null,
        "Name": "TEMPLA~1",

        "Location": null,
        "Comments": null,

        "ModificationTime": "10/21/2013 20:04:18.000000",
        "ShellItemTypeStr": "file_entry",
        "ExtentionBlockCount": 1,
        "Description": null,
        "FileSize": 0, A52A30:A63
```

```
        "FileSize": 0,
        "ExtentionBlocks": [
          {
            "LongName": "Templates",
            "ExtentionBlockSize": 68,

            "LocalizedName": null,
            "SeqNum": 0,

            "EntryNum": 253312,
            "FileReferenceInt": 253312,
            "AccessTime": "10/21/2013 04:00:00.000000",
            "CreationTime": "10/21/2013 20:16:24.000000",
            "Signature": "0xbeef0004L",
            "RefNum": "253312-0"
          }
        ]
      },

      {
        "ShellFolderId": null,

        "ShellItemTypeHex": "0x32L",
        "Identifier": null,
        "Name": "BUSINE~3.DOC",
        "Location": null,
        "Comments": null,

        "ModificationTime": "10/21/2013 19:47:30.000000",
        "ShellItemTypeStr": "file_entry",

        "ExtentionBlockCount": 1,
        "Description": null,
        "FileSize": 153600,
        "ExtentionBlocks": [
          {
```

```
            "LongName": "business_plan1.doc",
            "ExtentionBlockSize": 86,
            "LocalizedName": null,
            "SeqNum": 0,
            "EntryNum": 2494848,

            "FileReferenceInt": 2494848,
            "AccessTime": "10/21/2013 04:00:00.000000",

            "CreationTime": "10/21/2013
20:16:26.000000",
            "Signature": "0xbeef0004L",
            "RefNum": "2494848-0"
          }
        ]
      }
    ],
    "Volume": [
      {
        "ShellFolderId":
"00000000-0000-0000-0000-000000000000",
        "ShellItemTypeHex": "0x2fL",
        "Identifier":
"00000000-0000-0000-0000-000000000000",
        "Name": "F:\\",
        "Location": null,
        "Comments": null,
        "ModificationTime": null,

        "ShellItemTypeStr": "volume",
        "ExtentionBlockCount": 0,

        "Description": null,
        "FileSize": null,
        "ExtentionBlocks": []
      }
    ],
```

```
    "ParentLongName": "Templates",
    "ParentEntryNum": 253312,
    "DistinctTypesStr": "volume;root_folder;file_entry",
    "ExtentionListing": "0xbeef0004L;0xbeef0004L",
    "ItemCount": 5,

    "RootFolder": [
      {

        "ShellFolderId": "20d04fe0-3aea-1069-a2d8-08002b30309d",
        "ShellItemTypeHex": "0x1fL",
        "Identifier": null,
        "Name": null,
        "Location": null,
        "Comments": null,
        "ModificationTime": null,
        "ShellItemTypeStr": "root_folder",
        "ExtentionBlockCount": 0,

        "Description": null,
        "FileSize": null,

        "ExtentionBlocks": []
      }
    ]
  },
  "Description": null,

  "RelativePath": null,
  "Codepage": "cp1252",

  "IconLoc": null,
  "AppIdName": null,
  "FileExt": "doc",
  "NetworkPath": null,
  "FileSize": 153600,
  "CreationDateTime": "10/21/2013 20:16:24.870000",
  "EnvVarLoc": null
}
```

LINK FILE EXAMPLE

```
SELECT
linkfiles.DriveType,
linkfiles.VolumeLabel,
linkfiles.DriveSerialNumber,
json_extract(entry_item.value,'$.ExtentionBlocks[0].LongName') AS LongName,
json_extract(entry_item.value,'$.ExtentionBlocks[0].EntryNum') AS EntryNum,
json_extract(entry_item.value,'$.ExtentionBlocks[0].SeqNum') AS SeqNum,
linkfiles.LocalPath,
json_extract(entry_item.value,'$.ExtentionBlocks[0].CreationTime') AS CreationTime,
json_extract(entry_item.value,'$.ExtentionBlocks[0].AccessTime') AS AccessTime,
linkfiles.FileSize,
linkfiles.Source,
json_extract(LnkTrgData,'$.FileEntries') AS LnkTrgData
FROM
"linkfiles",
json_each(
    json_extract(LnkTrgData,'$.FileEntries')
) AS entry_item
WHERE
DriveType == 'DRIVE_REMOVABLE;'
```

RESULT

DriveType	VolumeLabel	DriveSerialNumber	LongName	EntryNum	SeqNum	LocalPath	CreationTime	AccessTime	File
DRIVE_REMOVABLE;	FILES	dc99-0719	9E9BFE4FBDC44D4A9F8491EC7F0ABDFD (1).vcs	15257984	0	E:\9E9BFE4FBDC44D4A9F8491EC7F0ABDFD (1).vcs	10/18/2013 18:43:42.000001	10/18/2013 04:00:00.000001	2576
DRIVE_REMOVABLE;	BLAKE FILES	944e-9b06	BetterWidgets Business Plan	255072	0	E:\BetterWidgets Business Plan	10/17/2013 21:06:46.000001	10/17/2013 04:00:00.000001	0
DRIVE_REMOVABLE;	USB	39c7-1beb	Business Plan for a Startup Business_0.doc	250944	0	F:\Business Plan for a Startup Business_0.doc	10/21/2013 18:53:02.000001	10/21/2013 04:00:00.000001	2355
DRIVE_REMOVABLE;	USB	39c7-1beb	Templates	253312	0	F:\Templates\business_plan1.doc	10/21/2013 20:16:24.000001	10/21/2013 04:00:00.000001	1536
DRIVE_REMOVABLE;	USB	39c7-1beb	business_plan1.doc	2494848	0	F:\Templates\business_plan1.doc	10/21/2013 20:16:26.000001	10/21/2013 04:00:00.000001	1536
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	From Donald's Windows Phone	66912	0	E:\From Donald's Windows Phone\Saved pictures\imagesCAL5YVMT.jpg	10/17/2013 19:29:06.000001	10/17/2013 04:00:00.000001	4263
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	Saved pictures	4309184	0	E:\From Donald's Windows Phone\Saved pictures\imagesCAL5YVMT.jpg	10/17/2013 19:29:12.000001	10/17/2013 04:00:00.000001	4263
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	imagesCAL5YVMT.jpg	50176224	0	E:\From Donald's Windows Phone\Saved pictures\imagesCAL5YVMT.jpg	10/17/2013 19:29:12.000001	10/17/2013 04:00:00.000001	4263
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	From Donald's Windows Phone	66912	0	E:\From Donald's Windows Phone\Saved pictures	10/17/2013 19:29:06.000001	10/17/2013 04:00:00.000001	0
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	Saved pictures	4309184	0	E:\From Donald's Windows Phone\Saved pictures	10/17/2013 19:29:12.000001	10/17/2013 04:00:00.000001	0
DRIVE_REMOVABLE;	USB	39c7-1beb	Templates	253312	0	F:\Templates	10/21/2013 20:16:24.000001	10/21/2013 04:00:00.000001	0
DRIVE_REMOVABLE;	PHOTOS BACK	440f-17ad	WP_20130803_001.jpg	66112	0	E:\WP_20130803_001.jpg	10/17/2013 19:29:04.000001	10/17/2013 04:00:00.000001	2842

DEMO

- Correlation of Links and Shellbags
- Get GcLinkParser at https://github.com/devgc/GcLinkParser
  - It will output into SQLite for you!

MFT EXAMPLE – JSON COLUMNS

mfth_magic	mfth_lsn	mfth_seq	mfth_flags_str	mfth_allocation	mfth_entry	mfth_entry_ref	mft_headers	attr_standardinformation	attr_filename	attr_data
FILE	24578749660	3	Folder	Allocated	200	200-3	[{"mfth_alloc_size": 1024, "mfth_allocation": "Allocated", "mfth_attr_ofs": 56, "mfth_base_rec": 0, "mfth_base_ref": "0-0", "mfth_base_seq": 0, "mfth_entry": 200, "mfth_entry_ref": "200-3", "mfth_flags": 3, "mfth_flags_str": "Folder", "mfth_link_cnt": 2, "mfth_lsn": 24578749660, "mfth_magic": "FILE", "mfth_next_attrid": 4, "mfth_padding1": "0000", "mfth_seq": 3, "mfth_update_cnt": 3, "mfth_update_ofs": 48, "mfth_us_array": ["0300", "0000", "0000"], "mfth_us_val": "0900", "mfth_used_size": 776}]	[{"contents": {"siattr_atime": "2013-09-26T18:26:42.956691", "siattr_attr_num": null, "siattr_class_id": 0, "siattr_ctime": "2013-09-26T18:26:42.956691", "siattr_dos": "", "siattr_maxver": 0, "siattr_mftmtime": "2013-09-26T18:26:42.956691", "siattr_mtime": "2013-09-26T18:26:42.956691", "siattr_own_id": 0, "siattr_quota": 0, "siattr_sec_id": 269, "siattr_usn": 9172738280, "siattr_ver": 0}, "header": {"attr_alloc_size": null, "attr_compress_size": null, "attr_content_ofs": 24, "attr_content_size": 72, "attr_flags": "", "attr_id": 0, "attr_index_flag": 0, "attr_init_size": null, "attr_last_vcn": null, "attr_len": 96, "attr_name_len": 0, "attr_name_ofs": 0, "attr_padding1": 0, "attr_padding2": null, "attr_real_size": null, "attr_res": 0, "attr_run_ofs": null, "attr_start_vcn": null, "attr_type": 16}}]	[{"contents": {"fnattr_alloc_fsize": 0, "fnattr_atime": "2013-09-26T18:26:42.956691", "fnattr_ctime": "2013-09-26T18:26:42.956691", "fnattr_flags": "Directory;", "fnattr_fullname": "000C0C~1", "fnattr_len_name": 8, "fnattr_mftmtime": "2013-09-26T18:26:42.956691", "fnattr_mtime": "2013-09-26T18:26:42.956691", "fnattr_name": "000C0C~1", "fnattr_namespace": 2, "fnattr_parent_rec": 192, "fnattr_parent_ref": "192-4", "fnattr_parent_seq": 4, "fnattr_real_fsize": 0}, "fullname": "\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Configuratio#\\", "header": {"attr_alloc_size": null, "attr_compress_size": null, "attr_content_ofs": 24, "attr_content_size": 82, "attr_flags": "", "attr_id": 3, "attr_index_flag": 1, "attr_init_size": null, "attr_last_vcn": null, "attr_len": 112, "attr_name_len": 0, "attr_name_ofs": 0, "attr_padding1": 0, "attr_padding2": null, "attr_real_size": null, "attr_res": 0, "attr_run_ofs": null, "attr_start_vcn": null, "attr_type": 48}}, {"contents": {"fnattr_alloc_fsize": 0, "fnattr_atime": "2013-09-26T18:26:42.956691", "fnattr_ctime": "2013-09-26T18:26:42.956691", "fnattr_flags": "Directory;", "fnattr_fullname": "000c0cc1624e7bef48ab396be286c2bf", "fnattr_len_name": 32, "fnattr_mftmtime": "2013-09-26T18:26:42.956691", "fnattr_mtime": "2013-09-26T18:26:42.956691", "fnattr_name": "000c0cc1624e7bef48ab396be286c2bf", "fnattr_namespace": 1, "fnattr_parent_rec": 192, "fnattr_parent_ref": "192-4", "fnattr_parent_seq": 4, "fnattr_real_fsize": 0}, "fullname": "\\Windows\\assembly\\NativeImages_v2.0.50727_32\\System.Configuratio#\\", "header": {"attr_alloc_size": null, "attr_compress_size": null, "attr_content_ofs": 24, "attr_content_size": 130, "attr_flags": "", "attr_id": 2, "attr_index_flag": 1, "attr_init_size": null, "attr_last_vcn": null, "attr_len": 160, "attr_name_len": 0, "attr_name_ofs": 0, "attr_padding1": 0, "attr_padding2": null, "attr_real_size": null, "attr_res": 0, "attr_run_ofs": null, "attr_start_vcn": null, "attr_type": 48}}]	

MFT FILELIST EXAMPLE

```
SELECT DISTINCT
coalesce(json_extract(fnattr.value,'$.fullname'),'') ||
   json_extract(fnattr.value,'$.contents.fnattr_name') ||
   coalesce(':' || json_extract(dtattr.value,'$.contents.daattr_stream_name'),'')
   AS filename,
mft_records.mfth_entry,
mft_records.mfth_seq,
mft_records.mfth_allocation,
CASE
WHEN (json_extract(dtattr.value,'$.contents.daattr_resident') IS 0)
            THEN json_extract(dtattr.value,'$.header.attr_content_size')
ELSE
  json_extract(dtattr.value,'$.contents.daattr_real_size')
END AS daattr_real_size,
json_extract(dtattr.value,'$.contents.daattr_stream_name') AS daattr_stream_name,
json_extract(dtattr.value,'$.contents.daattr_resident') AS daattr_resident,
json_extract(siattr.value,'$.contents.siattr_ctime') AS siattr_ctime,
json_extract(siattr.value,'$.contents.siattr_mtime') AS siattr_mtime,
json_extract(siattr.value,'$.contents.siattr_mftmtime') AS siattr_mftmtime,
json_extract(siattr.value,'$.contents.siattr_atime') AS siattr_atime,
json_extract(fnattr.value,'$.contents.fnattr_ctime') AS fnattr_ctime,
json_extract(fnattr.value,'$.contents.fnattr_mtime') AS fnattr_mtime,
json_extract(fnattr.value,'$.contents.fnattr_mftmtime') AS fnattr_mftmtime,
json_extract(fnattr.value,'$.contents.fnattr_atime') AS fnattr_atime,
json_extract(fnattr.value,'$.contents.fnattr_flags') AS fnattr_flags,
json_extract(fnattr.value,'$.contents.fnattr_name') AS fnattr_name,
json_extract(fnattr.value,'$.contents.fnattr_namespace') AS fnattr_namespace,
json_extract(fnattr.value,'$.contents.fnattr_parent_rec') AS fnattr_parent_rec,
json_extract(fnattr.value,'$.contents.fnattr_parent_seq') AS fnattr_parent_seq,
json_extract(dtattr.value,'$.contents.daattr_name') AS daattr_name,
json_extract(dtattr.value,'$.contents.daattr_real_size') AS daattr_real_size,
mft_records.info_source_file
FROM
"mft_records",
json_each(mft_records.attr_filename) as fnattr,
json_each(mft_records.attr_standardinformation) as siattr,
json_each(mft_records.attr_data) as dtattr;
```

RESULT

filename	mfth_entry	mfth_seq	mfth_allocation	daattr_real_size	daattr_stream_name	daattr_resident	siattr_ctime	siattr_mtime
\$MFT	0	1	Allocated	300679168	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$MFTMirr	1	1	Allocated	4096	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$LogFile	2	2	Allocated	67108864	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$Volume	3	3	Allocated	0	(Null)	0	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$AttrDef	4	4	Allocated	2560	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$Bitmap	6	6	Allocated	1712704	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$Boot	7	7	Allocated	8192	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$BadClus	8	8	Allocated	0	(Null)	0	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$BadClus:$Bad	8	8	Allocated	56121880576	$Bad	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$UpCase	10	10	Allocated	131072	(Null)	1	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$UpCase:$Info	10	10	Allocated	32	$Info	0	2013-06-02T03:43:28.889595	2013-06-02T03:43:28.88959
\$Extend\$RmMetadata\$Repair	28	1	Allocated	0	(Null)	1	2013-06-02T03:43:29.633318	2013-06-02T03:43:29.63331
\$Extend\$RmMetadata\$Repair:$Config	28	1	Allocated	8	$Config	0	2013-06-02T03:43:29.633318	2013-06-02T03:43:29.63331
\$Extend\$RmMetadata\$Repair:$Corrupt	28	1	Allocated	8388608	$Corrupt	1	2013-06-02T03:43:29.633318	2013-06-02T03:43:29.63331
\$Extend\$RmMetadata\$Repair:$Verify	28	1	Allocated	1048576	$Verify	1	2013-06-02T03:43:29.633318	2013-06-02T03:43:29.63331
\$Extend\$RmMetadata\$TxfLog\$Tops	31	1	Allocated	100	(Null)	0	2013-06-02T03:43:29.633318	2013-06-02T03:43:29.63331

MORE THOUGHTS

- SQLite works, but is probably not the best solution
- Need something like an embeddable MongoDB
- Technologies to look into
  - RocksDB (key value store database) [http://rocksdb.org/]
  - ObjectPath (query language for semi-structured data) [http://objectpath.org/]
  - Zorba (Zorba is a query processor designed for flexible data:
    from the simplicity of JSON to the completeness of XML.) [http://www.zorba.io/home]

QUESTIONS?

- Email us:
  - Matt: mseyer@g-cpartners.com
  - Dave: dcowen@g-cpartners.com
- Tweet us:
  - @forensic_matt
  - @hecfblog
- Get the code!
  - https://github.com/devgc