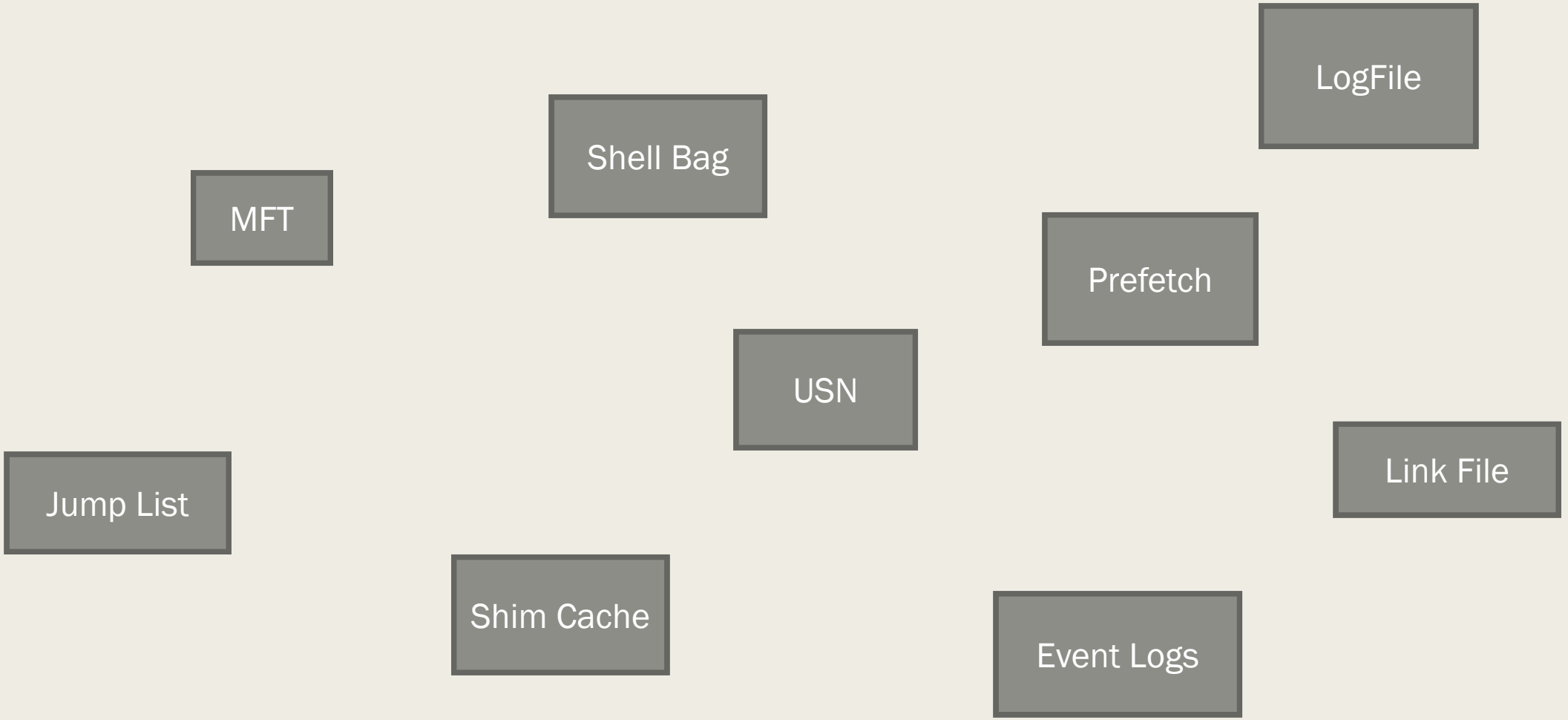
A DATABASE FOR FORENSICS

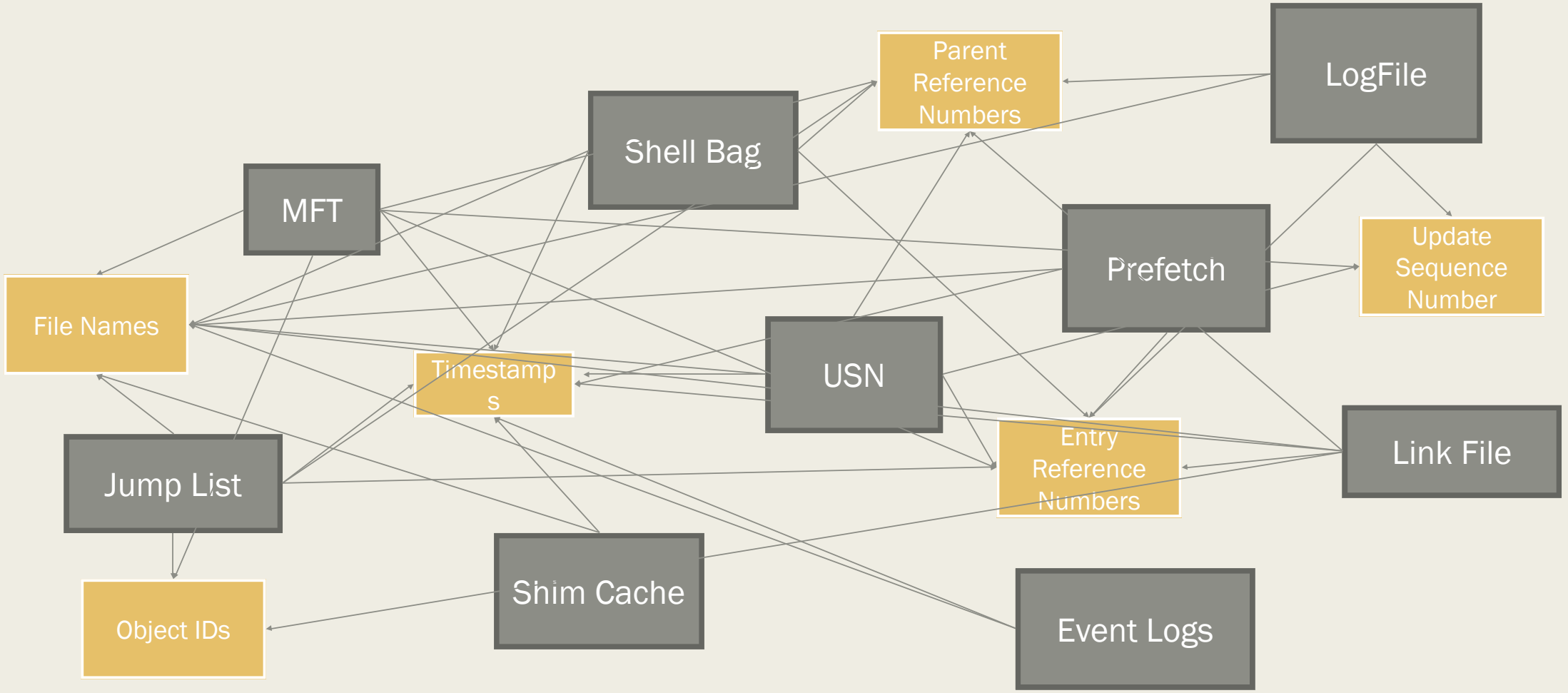
Artifact Correlation with ArangoDB

David Cowen & Matthew Seyer
G-C Partners, LLC

Lots of Artifacts



Lots of Correlation



The Process

- The better the tool output, the better the analysis
- The better the analysis, the better the report

Tool and Output Challenge

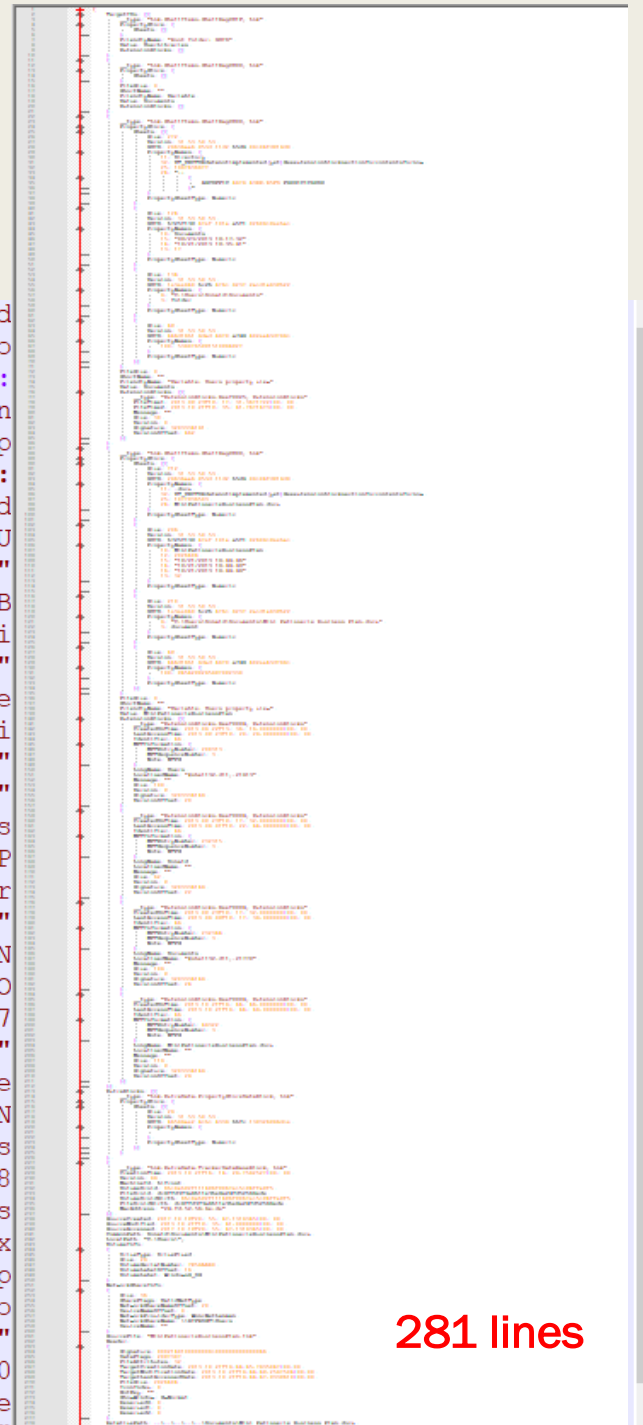
- The Forensic tool has to give us all the artifact!
- Output for People
  - *Linear*
  - *Easy to read*
- Output for Analysis
  - *Nested*
  - *Difficult to read with the human eye*
  - *More data for analysis*

Output for Human

	A	H	I	J	K	L	M	N	O	P	Q
1	SourceFile	FileSize	RelativePath	WorkingDirectory	FileAttributes	HeaderFlags	DriveType	VolumeSerialI	VolumeLabel	LocalPath	CommonPath
2	Mini Patisserie Business Plan.In	2026404	..\..\..\..\..\Docume	C:\Users\Donald\Documents	FileAttributeArchive	HasTargetIdList, HasL	Fixed storage media (Hard drive	7E58AAB0	Windows8_OS	C:\Users\	Donald\Documents\Mini Patisserie
3											

Output for Analysis


```
{"TargetIDs":[{"__type":"Lnk.ShellItems.ShellBag0X1F, Lnk","PropertyStore":{"Sheets":[]},"FriendlyName":"Root fold
"ExtensionBlocks":[]},{"__type":"Lnk.ShellItems.ShellBag0X00, Lnk","PropertyStore":{"Sheets":[]},"FileSize":0,"Sho
,"Value":"Documents","ExtensionBlocks":[]},{"__type":"Lnk.ShellItems.ShellBag0X00, Lnk","PropertyStore":{"Sheets":
,"GUID":"28636aa6-953d-11d2-b5d6-00c04fd918d0","PropertyNames":{"11":"Directory","32":"VT_VECTOR data not implemen
section for contents for now","25":"1887436877","24":"::{A8CDFF1C-4878-43BE-B5FD-F8091C1C60D0}"},"PropertySheetTyp
"31-53-50-53","GUID":"b725f130-47ef-101a-a5f1-02608c9eebac","PropertyNames":{"10":"Documents","15":"09/23/2013 19:
"13":"17"},"PropertySheetType":"Numeric"},{"Size":134,"Version":"31-53-50-53","GUID":"1e3ee840-bc2b-476c-8237-2acd
"C:\\Users\\Donald\\Documents","3":"folder"},"PropertySheetType":"Numeric"},{"Size":49,"Version":"31-53-50-53","GU
"446d16b1-8dad-4870-a748-402ea43d788c","PropertyNames":{"100":"5380765991510984927"},"PropertySheetType":"Numeric"
"FriendlyName":"Variable: Users property view","Value":"Documents","ExtensionBlocks":[{"__type":"ExtensionBlocks.B
"FileTime1":"\/Date(1379963851367)\/","FileTime2":"\/Date(1382384141767)\/","Message":"","Size":30,"Version":0,"Si
462}]},{"__type":"Lnk.ShellItems.ShellBag0X00, Lnk","PropertyStore":{"Sheets":[{"Size":712,"Version":"31-53-50-53"
"28636aa6-953d-11d2-b5d6-00c04fd918d0","PropertyNames":{"11":".docx","32":"VT_VECTOR data not implemented (yet) Se
contents for now","25":"1077936503","24":"Mini Patisserie Business Plan.docx"},"PropertySheetType":"Numeric"},{"Si
"GUID":"b725f130-47ef-101a-a5f1-02608c9eebac","PropertyNames":{"10":"Mini Patisserie Business Plan","12":"2026404"
"10/21/2013 18:44:49","16":"10/21/2013 18:44:48","13":"32"},"PropertySheetType":"Numeric"},{"Size":210,"Version":"
"1e3ee840-bc2b-476c-8237-2acd1a839b22","PropertyNames":{"8":"C:\\Users\\Donald\\Documents\\Mini Patisserie Busines
"PropertySheetType":"Numeric"},{"Size":49,"Version":"31-53-50-53","GUID":"446d16b1-8dad-4870-a748-402ea43d788c","P
"9454290285897092330"},"PropertySheetType":"Numeric"}]},"FileSize":0,"ShortName":"","FriendlyName":"Variable: User
Patisserie Business Plan","ExtensionBlocks":[{"__type":"ExtensionBlocks.Beef0004, ExtensionBlocks","CreatedOnTime"
"LastAccessTime":"\/Date(1379964028000)\/","Identifier":46,"MFTInformation":{"MFTEntryNumber":200313,"MFTSequenceN
"Users","LocalisedName":"@shell32.dll,-21813","Message":"","Size":100,"Version":9,"Signature":3203334148,"VersionO
"ExtensionBlocks.Beef0004, ExtensionBlocks","CreatedOnTime":"\/Date(1379963852000)\/","LastAccessTime":"\/Date(137
"MFTInformation":{"MFTEntryNumber":232315,"MFTSequenceNumber":3,"Note":"NTFS"},"LongName":"Donald","LocalisedName"
:9,"Signature":3203334148,"VersionOffset":22},{"__type":"ExtensionBlocks.Beef0004, ExtensionBlocks","CreatedOnTime
"LastAccessTime":"\/Date(1375989458000)\/","Identifier":46,"MFTInformation":{"MFTEntryNumber":232344,"MFTSequenceN
"Documents","LocalisedName":"@shell32.dll,-21770","Message":"","Size":108,"Version":9,"Signature":3203334148,"Vers
"ExtensionBlocks.Beef0004, ExtensionBlocks","CreatedOnTime":"\/Date(1382381086000)\/","LastAccessTime":"\/Date(138
"MFTInformation":{"MFTEntryNumber":48322,"MFTSequenceNumber":3,"Note":"NTFS"},"LongName":"Mini Patisserie Business
"Message":"","Size":118,"Version":9,"Signature":3203334148,"VersionOffset":28}]}],"ExtraBlocks":[{"__type":"Lnk.Ex
,"PropertyStore":{"Sheets":[{"Size":28,"Version":"31-53-50-53","GUID":"46588ae2-4cbc-4338-bbfc-139326986dce","Prop
"Numeric"}]}},{"__type":"Lnk.ExtraData.TrackerDataBaseBlock, Lnk","CreationTime":"\/Date(1382372068758)\/","Versio
"VolumeDroid":"6bc0ab92f111496f9067ec5c94ffa9f5","FileDroid":"dc8ffd3f3a6b11e3be8a24fd52566ede","VolumeDroidBirth"
"FileDroidBirth":"dc8ffd3f3a6b11e3be8a24fd52566ede","MacAddress":"24:fd:52:56:6e:de"}],"SourceCreated":"\/Date(150
"\/Date(1382384141000)\/","SourceAccessed":"\/Date(1507668947131)\/","CommonPath":"Donald\\Documents\\Mini Patisse
```

281 lines

Analysis Challenges

- Navigating the data
- Searching the data
- Correlating the data
- Formatting the data
- Automation of it all

Some History

- SQLite [SQL] – OSDFCON 2016
  - *Advantages*
    - Fast and local
  - *Disadvantages*
    - Not built for nested data (but possible to store)
    - Not efficient for joining on nested data (correlation)
    - Does not scale
- MongoDB [NoSQL]
  - *Advantages*
    - Built for nested data (JSON Documents)
  - *Disadvantages*
    - Server needed
    - Not relational

Some History

- Elasticsearch [Search Engine] - OSDFCON 2015
  - *Advantages*
    - Built for nested data (JSON Documents)
    - Super fast querying
  - *Disadvantages*
    - Not a database
    - Not relational
    - Server needed

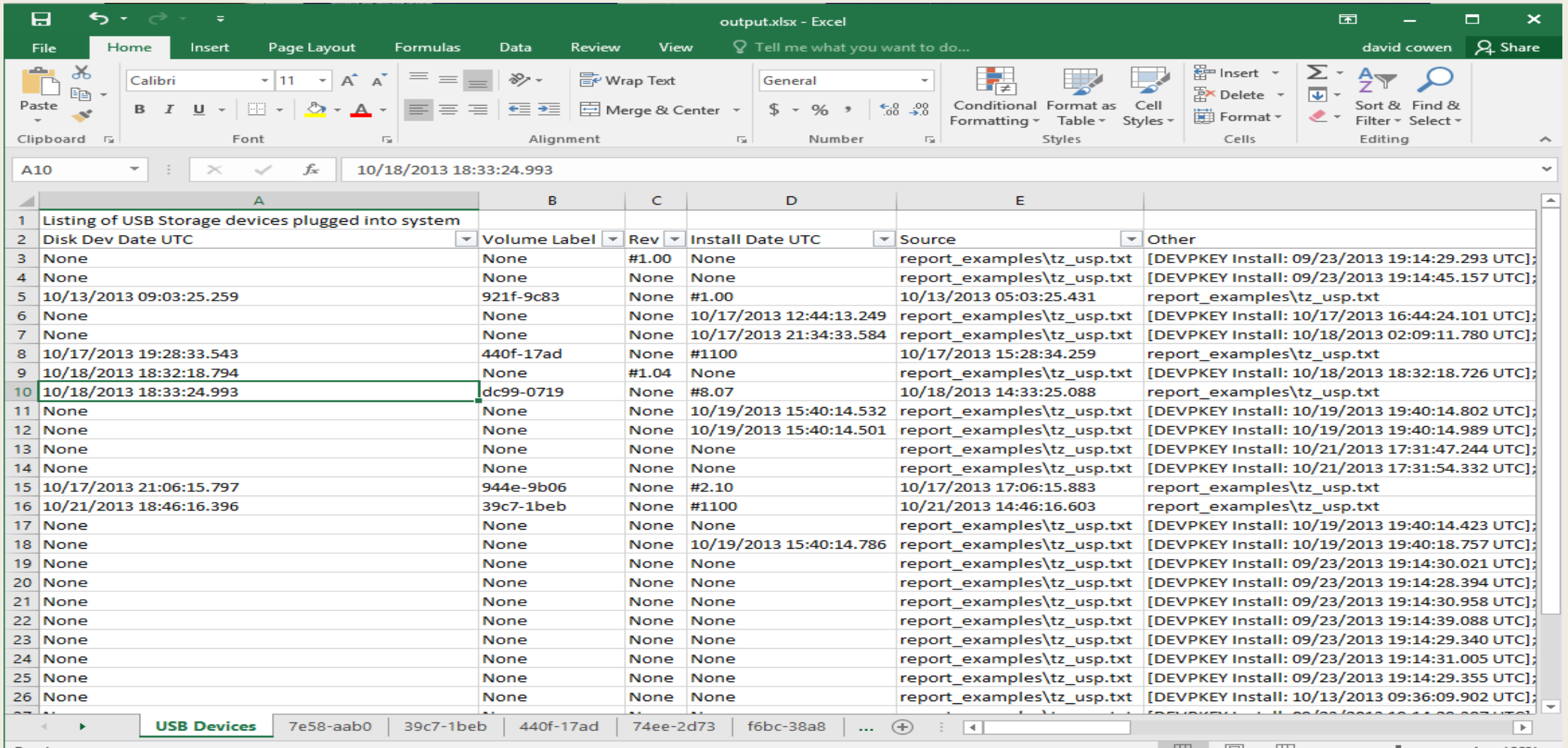
ArangoDB to the Rescue!

- Multi-Model Database
  - *Document Store (JSON)*
  - *Graph Database*
  - *Key-Value store*
- A great query language [AQL]
- Efficient relational queries on nested documents
- Written in C! AKA NO JAVA!
- Maintains a scalable environment
- JavaScript microservices
- Ships with a great interface

2015 Rewind Example
Device History in Elasticsearch

- 156 lines of python script to stich things together.
- To much code to display. See it here: https://github.com/devgc/ElasticHandler/blob/master/scripts/ExternalDeviceExample.py

Device History in Elasticsearch Result



output.xlsx - Excel

	A	B	C	D	E	
1	Listing of USB Storage devices plugged into system					
2	Disk Dev Date UTC	Volume Label	Rev	Install Date UTC	Source	Other
3	None	None	#1.00	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:29.293 UTC];
4	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:45.157 UTC];
5	10/13/2013 09:03:25.259	921f-9c83	None	#1.00	10/13/2013 05:03:25.431	report_examples\tz_usp.txt
6	None	None	None	10/17/2013 12:44:13.249	report_examples\tz_usp.txt	[DEVPKEY Install: 10/17/2013 16:44:24.101 UTC];
7	None	None	None	10/17/2013 21:34:33.584	report_examples\tz_usp.txt	[DEVPKEY Install: 10/18/2013 02:09:11.780 UTC];
8	10/17/2013 19:28:33.543	440f-17ad	None	#1100	10/17/2013 15:28:34.259	report_examples\tz_usp.txt
9	10/18/2013 18:32:18.794	None	#1.04	None	report_examples\tz_usp.txt	[DEVPKEY Install: 10/18/2013 18:32:18.726 UTC];
10	10/18/2013 18:33:24.993	dc99-0719	None	#8.07	10/18/2013 14:33:25.088	report_examples\tz_usp.txt
11	None	None	None	10/19/2013 15:40:14.532	report_examples\tz_usp.txt	[DEVPKEY Install: 10/19/2013 19:40:14.802 UTC];
12	None	None	None	10/19/2013 15:40:14.501	report_examples\tz_usp.txt	[DEVPKEY Install: 10/19/2013 19:40:14.989 UTC];
13	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 10/21/2013 17:31:47.244 UTC];
14	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 10/21/2013 17:31:54.332 UTC];
15	10/17/2013 21:06:15.797	944e-9b06	None	#2.10	10/17/2013 17:06:15.883	report_examples\tz_usp.txt
16	10/21/2013 18:46:16.396	39c7-1beb	None	#1100	10/21/2013 14:46:16.603	report_examples\tz_usp.txt
17	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 10/19/2013 19:40:14.423 UTC];
18	None	None	None	10/19/2013 15:40:14.786	report_examples\tz_usp.txt	[DEVPKEY Install: 10/19/2013 19:40:18.757 UTC];
19	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:30.021 UTC];
20	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:28.394 UTC];
21	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:30.958 UTC];
22	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:39.088 UTC];
23	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:29.340 UTC];
24	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:31.005 UTC];
25	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 09/23/2013 19:14:29.355 UTC];
26	None	None	None	None	report_examples\tz_usp.txt	[DEVPKEY Install: 10/13/2013 09:36:09.902 UTC];

USB Devices | 7e58-aab0 | 39c7-1beb | 440f-17ad | 74ee-2d73 | f6bc-38a8 | ...

2016 Rewind Example
SBAGS and LNKS in SQLite

```
CREATE TEMP TABLE linkpaths AS
	SELECT DISTINCT
		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;';
```

```
SELECT DISTINCT
	sbags.AbsolutePath,
	linkpaths.LocalPath AS "Lnk Local Path",
	linkpaths.DriveType,
	linkpaths.DriveSerialNumber,
	linkpaths.VolumeLabel,
	sbags.MFTEntry,
	CASE
		WHEN (sbags.MFTSequenceNumber IS NULL)
			THEN 0
		ELSE
			sbags.MFTSequenceNumber
		END AS MFTSeqNumber,
	sbags.MFTSequenceNumber,
	linkpaths.EntryNum,
	linkpaths.SeqNum,
	RTRIM(sbags.Value) AS SbagDirName,
	linkpaths.LongName AS LnkDirName,
	linkpaths.LnkTrgData,
	linkpaths.Source
FROM
	sbags
LEFT JOIN linkpaths ON (
	(sbags.MFTEntry = linkpaths.EntryNum) AND
	(MFTSeqNumber = linkpaths.SeqNum) AND
	(SbagDirName = linkpaths.LongName)
)
WHERE AbsolutePath NOT LIKE '%C:%'
ORDER BY "Lnk Local Path"
```

SBAGS and LNKS in SQLite Result

AbsolutePath	Lnk Local Path	DriveType	DriveSerialNumber	VolumeLabel	MFTEntry	MFTSeqNumber	MFTSequenceNumber	EntryNum	SeqNum	SbagDirName
Desktop\E:\\testfolder002	E:\testfolder002\testfile010.gif	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	113	1	1	113	1	testfolder002
Desktop\E:\\testfolder002	E:\testfolder002\testfile007.png	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	113	1	1	113	1	testfolder002
Desktop\E:\\testfolder002	E:\testfolder002	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	113	1	1	113	1	testfolder002
Desktop\My Computer\E:\testfolder001	E:\testfolder001\testfile054.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\E:\\testfolder001	E:\testfolder001\testfile054.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\My Computer\E:\testfolder001	E:\testfolder001\testfile030.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\E:\\testfolder001	E:\testfolder001\testfile030.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\My Computer\E:\testfolder001	E:\testfolder001\testfile024.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\E:\\testfolder001	E:\testfolder001\testfile024.html	DRIVE_REMOVABLE;	d2df-b1f3	RFMF	35	1	1	35	1	testfolder001
Desktop\E:\\stuff	E:\stuff\fsevent_files_2\0000000000005754	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	16778592	0		16778592	0	stuff
Desktop\E:\\stuff\fsevent_files_2	E:\stuff\fsevent_files_2\0000000000005754	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	17285376	0		17285376	0	fsevent_files_2
Desktop\E:\\stuff	E:\stuff\fsevent_files_2	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	16778592	0		16778592	0	stuff
Desktop\E:\\stuff\fsevent_files_2	E:\stuff\fsevent_files_2	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	17285376	0		17285376	0	fsevent_files_2
Desktop\E:\\stuff	E:\stuff\copy_test	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	16778592	0		16778592	0	stuff
Desktop\E:\\stuff\copy_test	E:\stuff\copy_test	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	17285216	0		17285216	0	copy_test
Desktop\E:\\events-1-11	E:\events-1-11\fseventsd-uuid	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	16777440	0		16777440	0	events-1-11
Desktop\E:\\events-1-11	E:\events-1-11	DRIVE_REMOVABLE;	d47c-d3e2	MACFILES	16777440	0		16777440	0	events-1-11
Desktop\My Computer\D:\stuff	D:\stuff\testfolder001	DRIVE_REMOVABLE;	8eba-8d18	STORE N GO	38	2	2	38	2	stuff
Desktop\My Computer\D:\stuff\testfolder001	D:\stuff\testfolder001	DRIVE_REMOVABLE;	8eba-8d18	STORE N GO	46	2	2	46	2	testfolder001

2017 Example
SBAGS and LNKS in ArangoDB

```
FOR lnk IN lnks
  FILTER lnk.LnkTrgData.FileEntries != null
  FILTER lnk.DriveType == "DRIVE_REMOVABLE;"
  FOR entry IN lnk.LnkTrgData.FileEntries
    FOR extention IN entry.ExtentionBlocks
      FILTER extention.LongName != null
      FOR shellbag IN sbags
        FILTER (shellbag.Value == extention.LongName &&
                TO_NUMBER(shellbag.MFTEntry) == extention.EntryNum &&
                TO_NUMBER(shellbag.MFTSequenceNumber) == extention.SeqNum)

        RETURN DISTINCT {
          "lnk.VolumeLabel": lnk.VolumeLabel,
          "lnk.DriveSerialNumber": lnk.DriveSerialNumber,
          "shellbag.AbsolutePath": shellbag.AbsolutePath,
          "extention.LongName": extention.LongName,
          "extention.RefNum": extention.RefNum
        }
```

SBAGS and LNKS in ArangoDB Result

lnk.VolumeLabel	lnk.DriveSerialNumber	shellbag.AbsolutePath	extention.LongName	extention.RefNun
STORE N GO	8eba-8d18	Desktop\My Computer\D:\stuff	stuff	38-2
STORE N GO	8eba-8d18	Desktop\D:\\stuff	stuff	38-2
STORE N GO	8eba-8d18	Desktop\D:\\stuff\some docs	some docs	39-2
MACFILES	d47c-d3e2	Desktop\E:\\stuff	stuff	16778592-0
MACFILES	d47c-d3e2	Desktop\E:\\stuff\fsevent_files_2	fsevent_files_2	17285376-0

*Shows us that Shell Bags “D:\stuff” is a different volume than “E:\stuff”

ArangoDB Query Example #2 Device History

```
FOR device IN usp
    FILTER device.`instance id/serial #` != "00000000"
    FOR event IN events
        // We need to make both the same CASE to insure contains match
        FILTER CONTAINS(UPPER(event.UserData),UPPER(device.`instance id/serial #`))
        // Sort by event time
        SORT event.System.TimeCreated.SystemTime
        RETURN {
            "time":DATE_FORMAT(event.System.TimeCreated.SystemTime,'%mm/%dd/%yyyy %hh:%ii:%ss.%fff'),
            "device":device.`device name`,
            "serial":device.`instance id/serial #`,
            "vid":device.vid,
            "pid":device.pid,
            "provider":event.System.Provider.Name,
            "event_id": event.System.EventID,
            "record_id": event.System.EventRecordID,
            "event":event
        }
```

Device History Result

time	device	serial	vid	pid	provider	event_id	record_id	event
10/18/2013 18:33:25.474	MBIL SSM Moser Baer Disk USB Device	mba34212080313074295&0	#1ec9	#a081	Microsoft-W	20003	6736	[object Object]
10/18/2013 18:33:26.235	MBIL SSM Moser Baer Disk USB Device	mba34212080313074295&0	#1ec9	#a081	Microsoft-W	20001	6739	[object Object]
10/19/2013 01:52:27.220	USB Composite Device	0x0001	#04f2	#b35e	Microsoft-W	500	2499	[object Object]
10/19/2013 02:05:23.476	USB Composite Device	0x0001	#04f2	#b35e	Microsoft-W	500	2534	[object Object]
10/19/2013 19:40:14.802	RM-860;Nokia Lumia 928	6&6d096df&0&0002	#0421	#0661	Microsoft-W	20001	6965	[object Object]
10/19/2013 19:40:14.974	RM-860;Nokia Lumia 928	6&6d096df&0&0001	#0421	#0661	Microsoft-W	20001	6966	[object Object]
10/19/2013 19:40:15.177	Donald's Windows Phone	6&6d096df&0&0000	#0421	#0661	Microsoft-W	10000	6967	[object Object]
10/19/2013 19:40:15.271	Donald's Windows Phone	6&6d096df&0&0000	#0421	#0661	Microsoft-W	20003	6971	[object Object]
10/19/2013 19:40:15.271	Donald's Windows Phone	6&6d096df&0&0000	#0421	#0661	Microsoft-W	20003	6970	[object Object]
10/19/2013 19:40:18.695	Donald's Windows Phone	6&6d096df&0&0000	#0421	#0661	Microsoft-W	205	9	[object Object]
10/19/2013 19:40:18.757	Donald's Windows Phone	6&6d096df&0&0000	#0421	#0661	Microsoft-W	20001	6975	[object Object]
10/21/2013 17:37:40.989	USB Composite Device	0x0001	#04f2	#b35e	Microsoft-W	500	2656	[object Object]
10/21/2013 18:46:17.237	SMI USB DISK USB Device	aa04012700011123&0	#090c	#1000	Microsoft-W	10000	7068	[object Object]
10/21/2013 18:46:17.393	SMI USB DISK USB Device	aa04012700011123&0	#090c	#1000	Microsoft-W	20003	7071	[object Object]
10/21/2013 18:46:17.704	SMI USB DISK USB Device	aa04012700011123&0	#090c	#1000	Microsoft-W	20001	7072	[object Object]
10/22/2013 21:41:53.951	FRESPONS TACTICAL_Subject USB Dev	00000022928277&0	#1307	#0116	Microsoft-W	10000	7141	[object Object]
10/22/2013 21:41:54.029	FRESPONS TACTICAL_Subject USB Dev	00000022928277&0	#1307	#0116	Microsoft-W	20003	7144	[object Object]
10/22/2013 21:41:54.373	FRESPONS TACTICAL_Subject USB Dev	00000022928277&0	#1307	#0116	Microsoft-W	20001	7147	[object Object]

DEMOS!

Questions

- Twitter
  - *@hecfblog*
  - *@forensic_matt*
- Blog
  - *http://www.hecfblog.com/*
- Code
  - *https://github.com/devgc*
  - *https://github.com/forensicmatt*