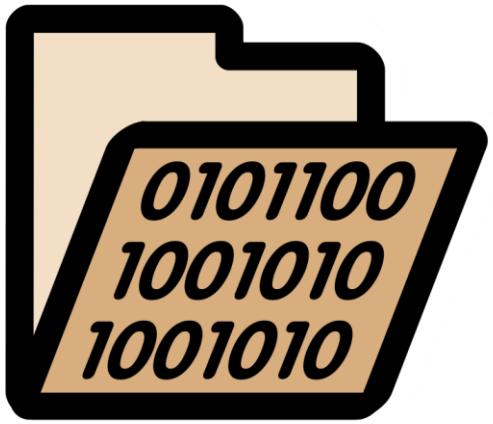
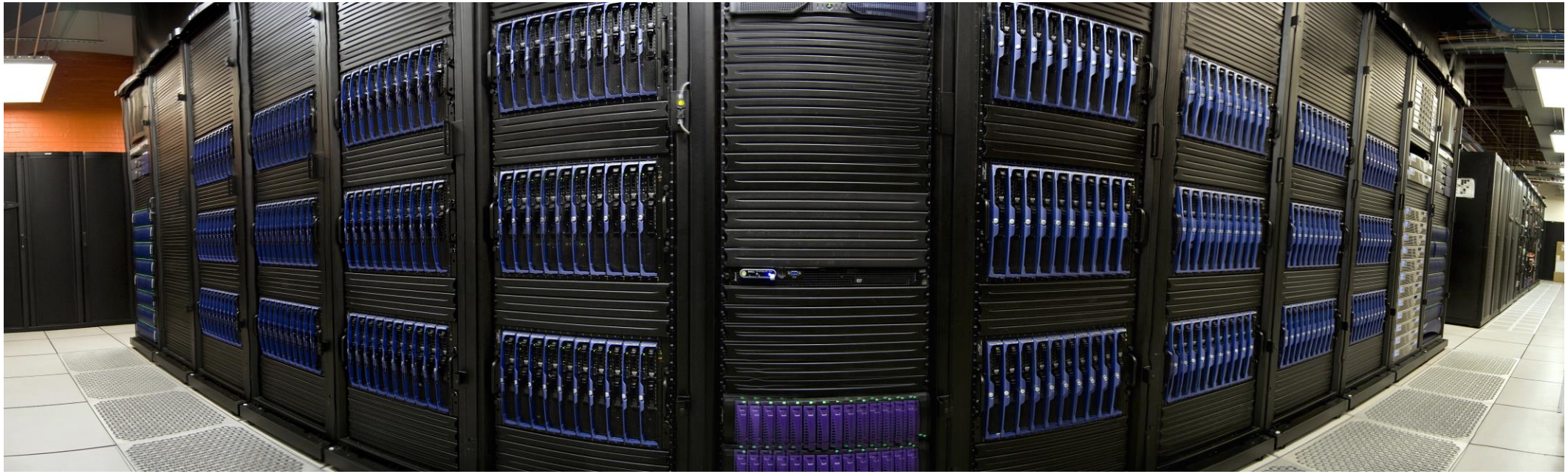
Power(Shell)ing Through the Timeline

DISK ARTIFACT ANALYSIS AT SCALE WITH KANSA

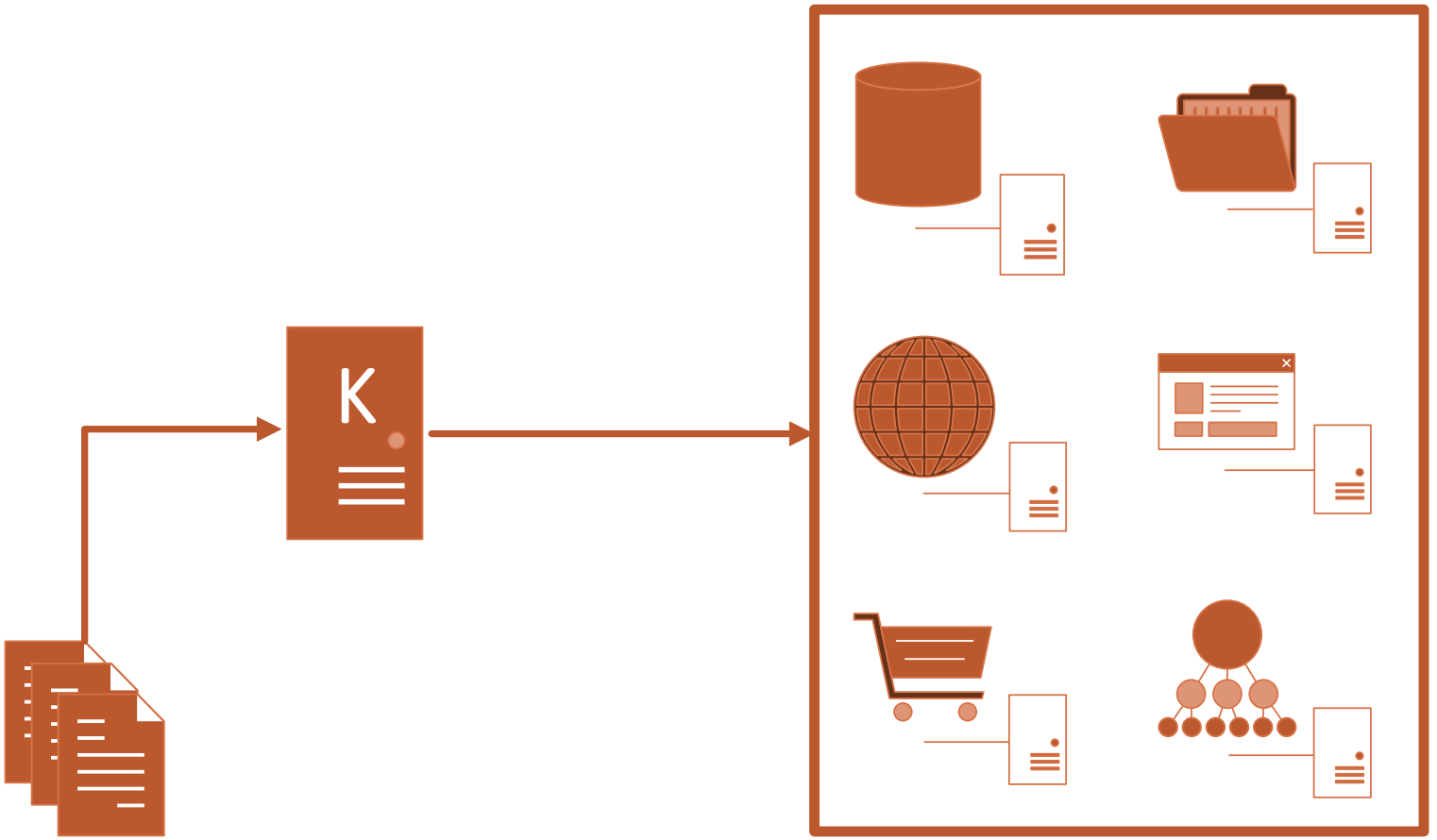
Tradition!



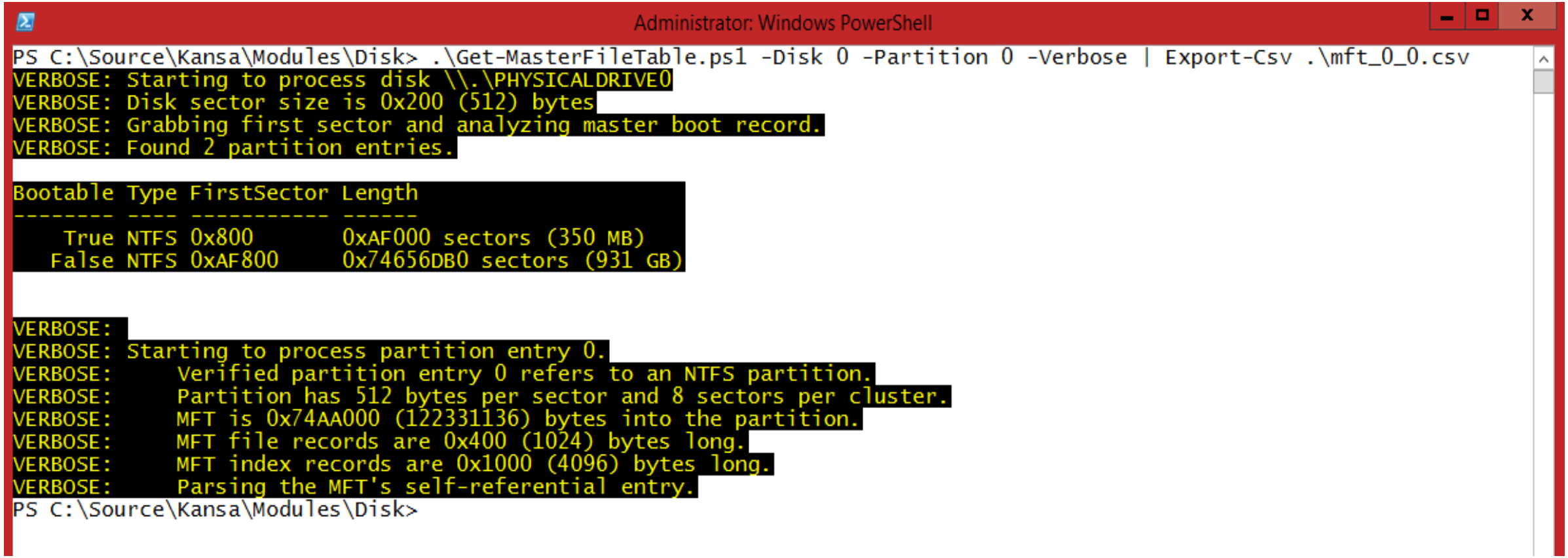
…but?



Kansa



Get-MasterFileTable.ps1



Why this way?

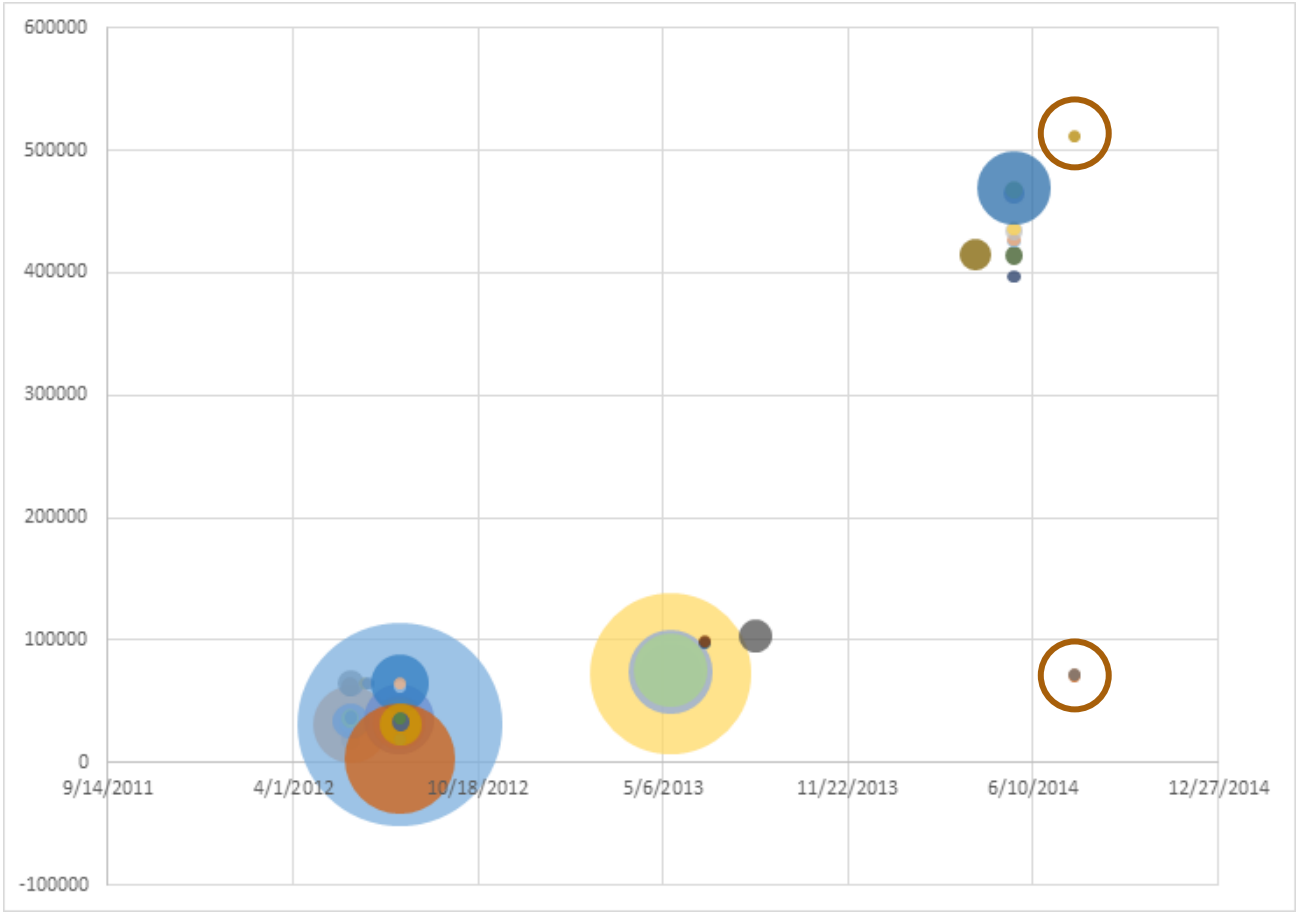
PowerShell is installed by default on all systems since Windows Vista with 3.0 and later available since Windows 7.

No need for third-party disk drivers that can introduce instability or other issues, and the project is open-source so you can verify the code before you run it.

Kansa is agentless, so there's nothing to install.

In short: If you're running Windows, you already have everything you need to use it.

Analysis


600000
500000
400000
300000
200000
100000
0
-100000
9/14/2011
4/1/2012
10/18/2012
5/6/2013
11/22/2013
6/10/2014
12/27/2014

Analysis

```
SELECT
        TO_DATE(TO_TIMESTAMP([StdInfo: Created], 'yyyy-MM-ddTHH:mm:ssZ')) AS [SI Created Date],
        QUANTIZE([Entry Number], 1000) AS [Entry Group],
        COUNT(*) AS [Row Count]
INTO %myOutput%
FROM %myInput%
WHERE EXTRACT_EXTENSION([File Name]) = '%myExtension%'
GROUP BY
        TO_DATE(TO_TIMESTAMP([StdInfo: Created], 'yyyy-MM-ddTHH:mm:ssZ')),
        QUANTIZE([Entry Number], 1000)
```

Analysis

Least-frequency analysis

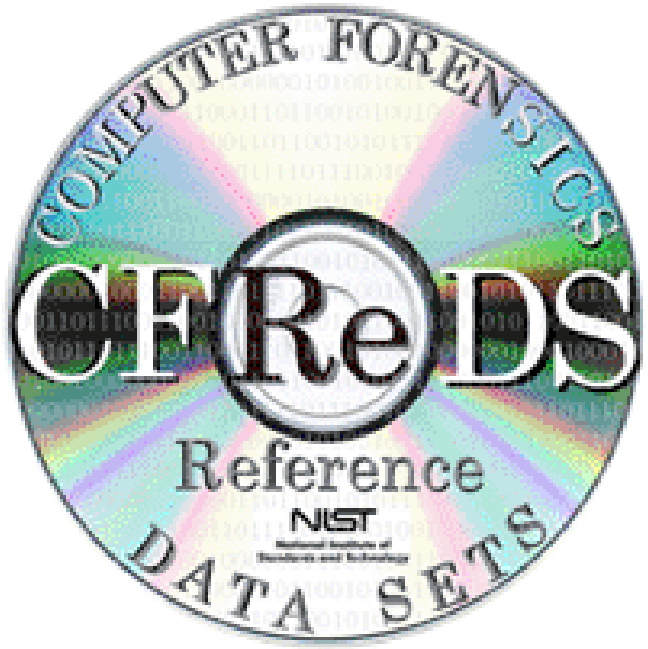
Large files (staged exfiltration)

Deleted executables

On-demand compiler residue

Etc…

Shortcomings & Future work



C#

Contact me!

Jon Turner

jturner@microsoft.com

@z4ns4tsu