When Malware Meets Murphy

Mattijs van Ommeren
Principal Consultant at Nixu

Hack In The Box Amsterdam
Commsec Track

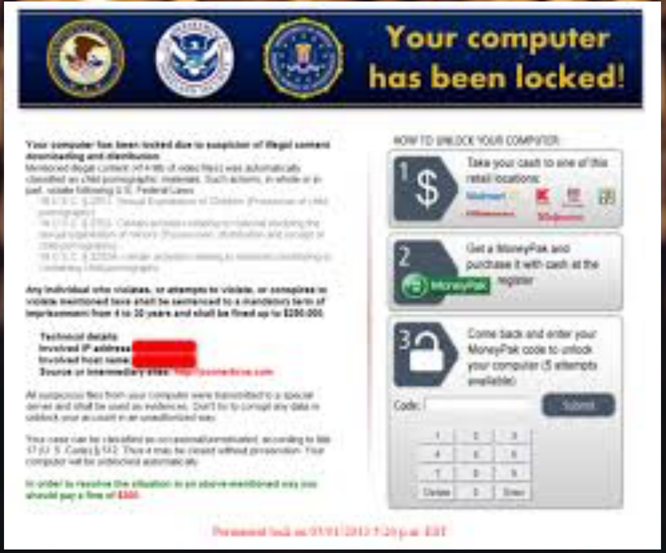
About Me

- Mattijs van Ommeren
- Principal Consultant at Nixu
- 15+ years experience in IT security
- Pentesting, incident handling, forensics, research

- Twitter: @alcyonsecurity
- E-mail: mattijs.vanommeren@nixu.com

The Bad Beginning

- First case of ransomware reported in 2005 (TROJ_CRYZIP.A)
- Since 2012 spread across Europe and the U.S.
- 2013: Cryptolocker



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

- 18 U.S.C. § 2251- Sexual Exploitation of Children (Possession of child pornography)
- 18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
- 18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://[illegible].com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

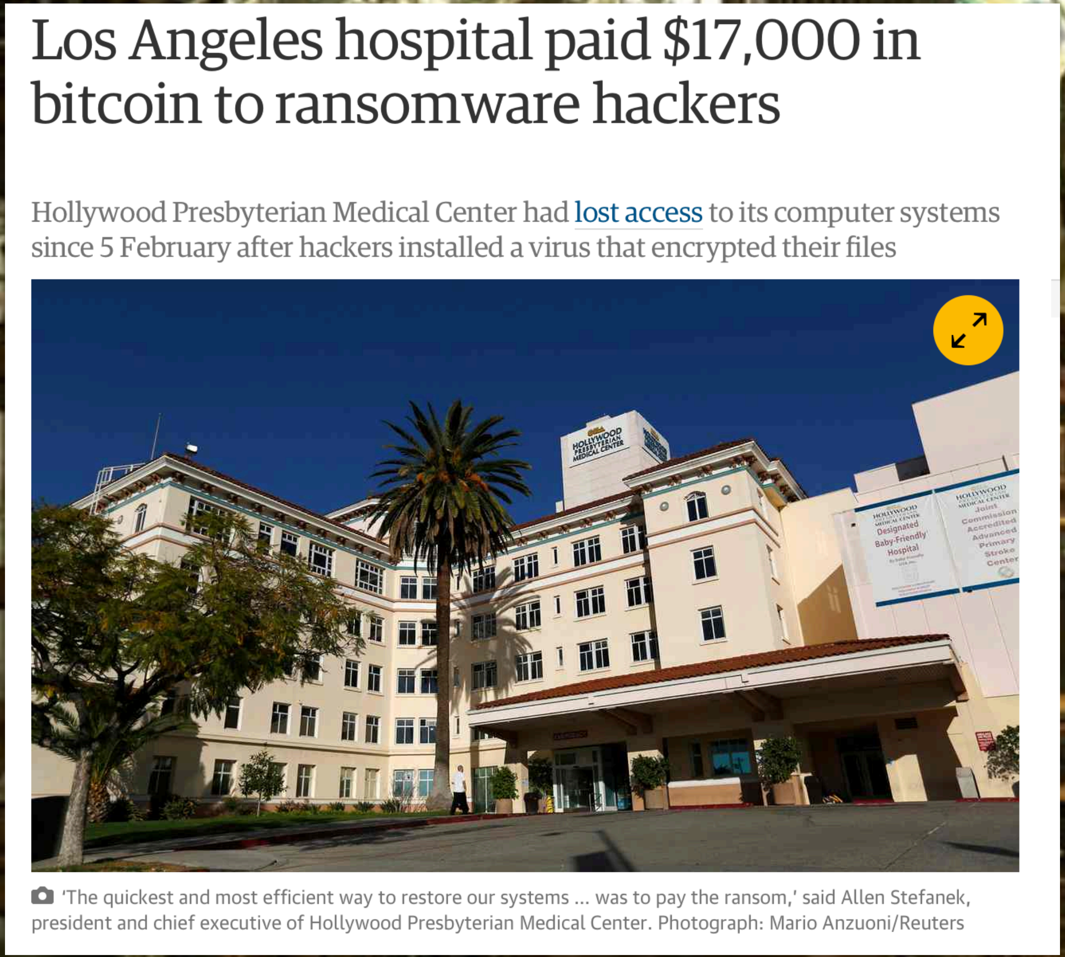
2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

Permanent lock at 07/01/2013 7:20 p.m. EST

The Hostile Hospital



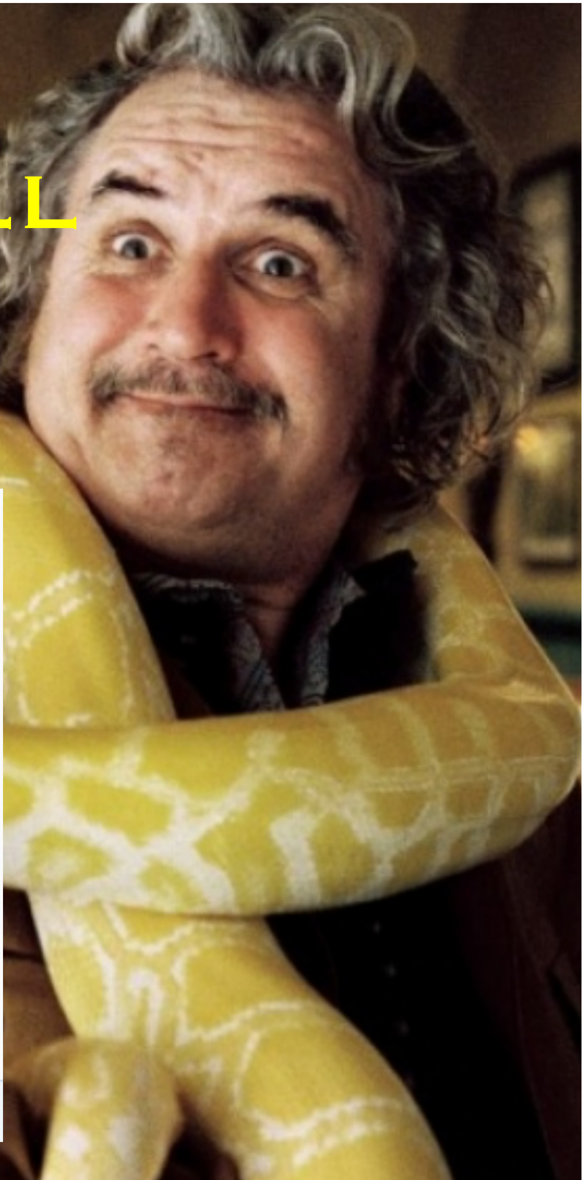
Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

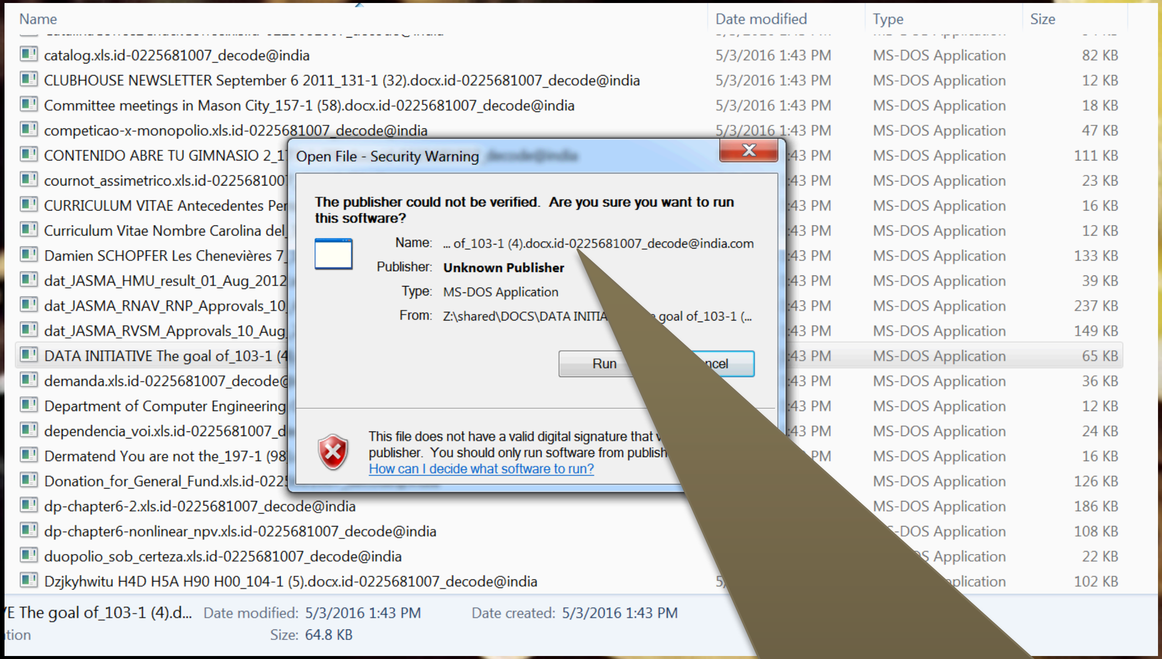
Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER
Designated Baby-Friendly Hospital
Joint Commission Accredited Advanced Primary Stroke Center

'The quickest and most efficient way to restore our systems … was to pay the ransom,' said Allen Stefanek, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni/Reuters

The Phone call





Name	Date modified	Type	Size
catalog.xls.id-0225681007_decode@india	5/3/2016 1:43 PM	MS-DOS Application	82 KB
CLUBHOUSE NEWSLETTER September 6 2011_131-1 (32).docx.id-0225681007_decode@india	5/3/2016 1:43 PM	MS-DOS Application	12 KB
Committee meetings in Mason City_157-1 (58).docx.id-0225681007_decode@india	5/3/2016 1:43 PM	MS-DOS Application	18 KB
competicao-x-monopolio.xls.id-0225681007_decode@india	5/3/2016 1:43 PM	MS-DOS Application	47 KB
CONTENIDO ABRE TU GIMNASIO 2_1	:43 PM	MS-DOS Application	111 KB
cournot_assimetrico.xls.id-0225681007	:43 PM	MS-DOS Application	23 KB
CURRICULUM VITAE Antecedentes Per	:43 PM	MS-DOS Application	16 KB
Curriculum Vitae Nombre Carolina del	:43 PM	MS-DOS Application	12 KB
Damien SCHOPFER Les Chenevières 7	:43 PM	MS-DOS Application	133 KB
dat_JASMA_HMU_result_01_Aug_2012	:43 PM	MS-DOS Application	39 KB
dat_JASMA_RNAV_RNP_Approvals_10	:43 PM	MS-DOS Application	237 KB
dat_JASMA_RVSM_Approvals_10_Aug	:43 PM	MS-DOS Application	149 KB
DATA INITIATIVE The goal of_103-1 (4	:43 PM	MS-DOS Application	65 KB
demanda.xls.id-0225681007_decode@	:43 PM	MS-DOS Application	36 KB
Department of Computer Engineering	:43 PM	MS-DOS Application	12 KB
dependencia_voi.xls.id-0225681007_d	:43 PM	MS-DOS Application	24 KB
Dermatend You are not the_197-1 (98	PM	MS-DOS Application	16 KB
Donation_for_General_Fund.xls.id-022		MS-DOS Application	126 KB
dp-chapter6-2.xls.id-0225681007_decode@india		MS-DOS Application	186 KB
dp-chapter6-nonlinear_npv.xls.id-0225681007_decode@india		-DOS Application	108 KB
duopolio_sob_certeza.xls.id-0225681007_decode@india		S Application	22 KB
Dzjkyhwitu H4D H5A H90 H00_104-1 (5).docx.id-0225681007_decode@india	5	plication	102 KB

E The goal of_103-1 (4).d... Date modified: 5/3/2016 1:43 PM Date created: 5/3/2016 1:43 PM
tion Size: 64.8 KB

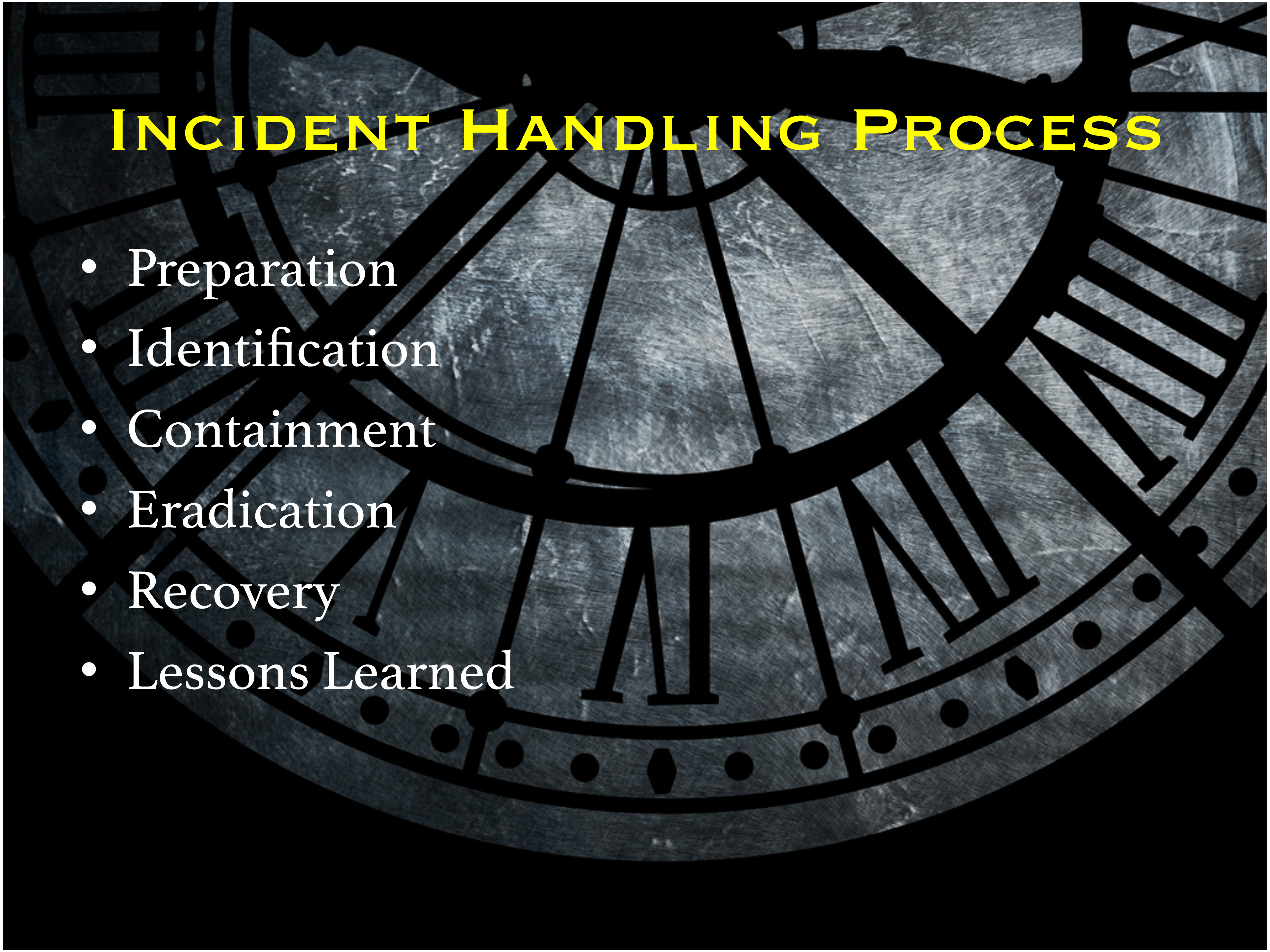
Open File - Security Warning [redacted]

The publisher could not be verified. Are you sure you want to run this software?

Name: ... of_103-1 (4).docx.id-0225681007_decode@india.com
Publisher: **Unknown Publisher**
Type: MS-DOS Application
From: Z:\shared\DOCS\DATA INITIA goal of_103-1 (...

This file does not have a valid digital signature that
publisher. You should only run software from publish
How can I decide what software to run?

The goal_of_103.docx.id-0225681007_decode@india.com



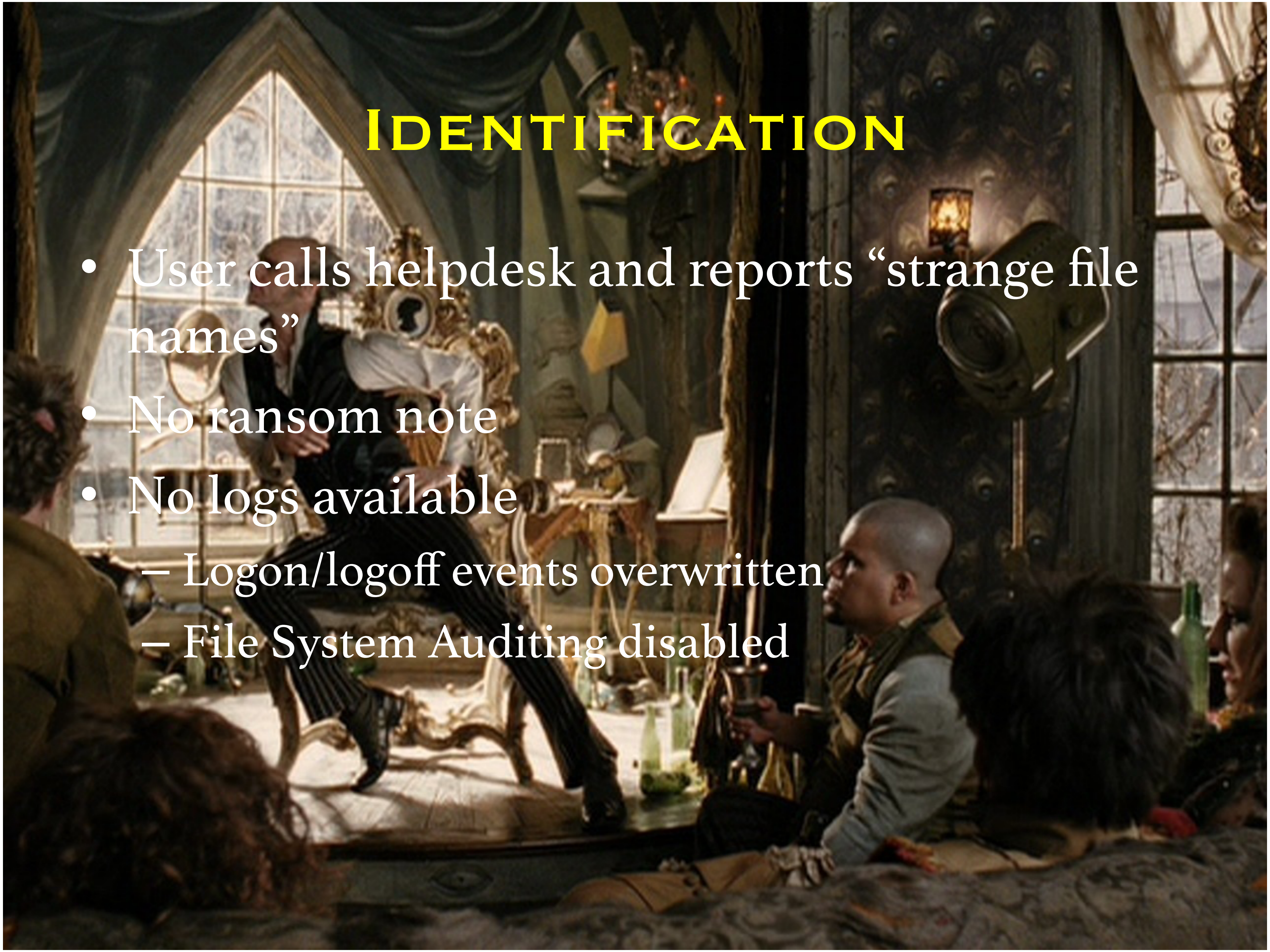
Incident Handling Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Preparation

- Policy
- Response Plan
- Communication Plan
- Documentation
- Access Control
- Tools
- Training

Identification



- User calls helpdesk and reports “strange file names”
- No ransom note
- No logs available
  - Logon/logoff events overwritten
  - File System Auditing disabled

Encryption in progress

- Active SMB session:
  - Netstat - ESTABLISHED 445/TCP
  - OPENFILES.EXE
  - Powershell Get-SMBOpenFile (Windows 2012 R2)
- Less volatile
  - Firewall connection logs
  - NETFLOW data

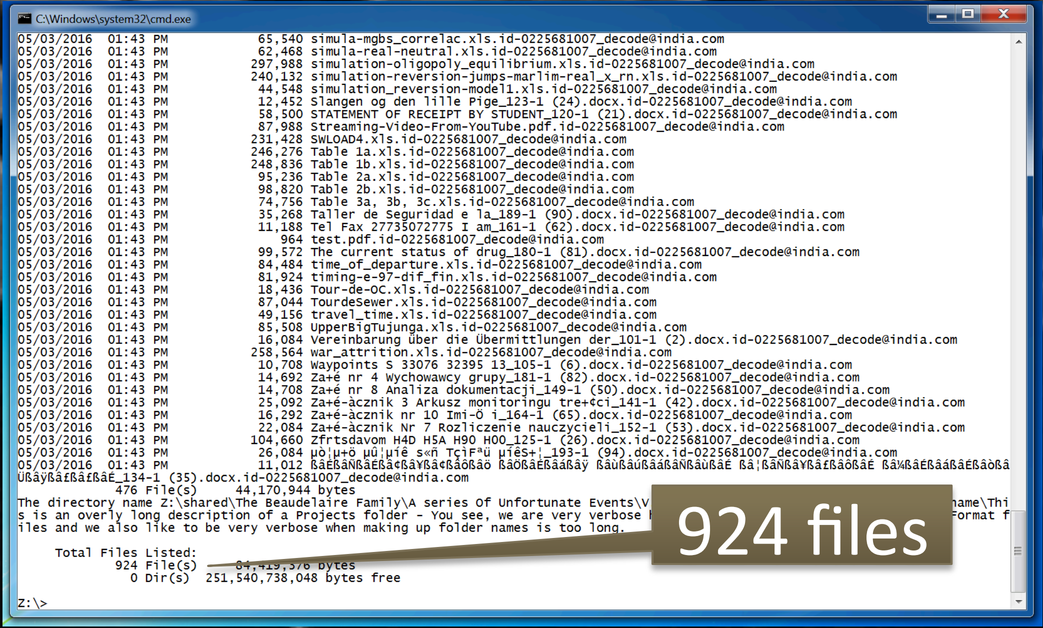
Containment

- Prevent it from getting worse
  - – Unplug the network cable?
  - – Set file shares to Read-only access
  - – File/Share Canary
    - FSRM File Screen (Windows 2008 and up) https://community.spiceworks.com/how_to/100368-cryptolocker-canary-detect-it-early
    - File System Audit & Sinkhole http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html
  - – Block C2 traffic

Which Files?

- Easily identifiable through new file extension

```
dir /s /a *_decode@india.com
```

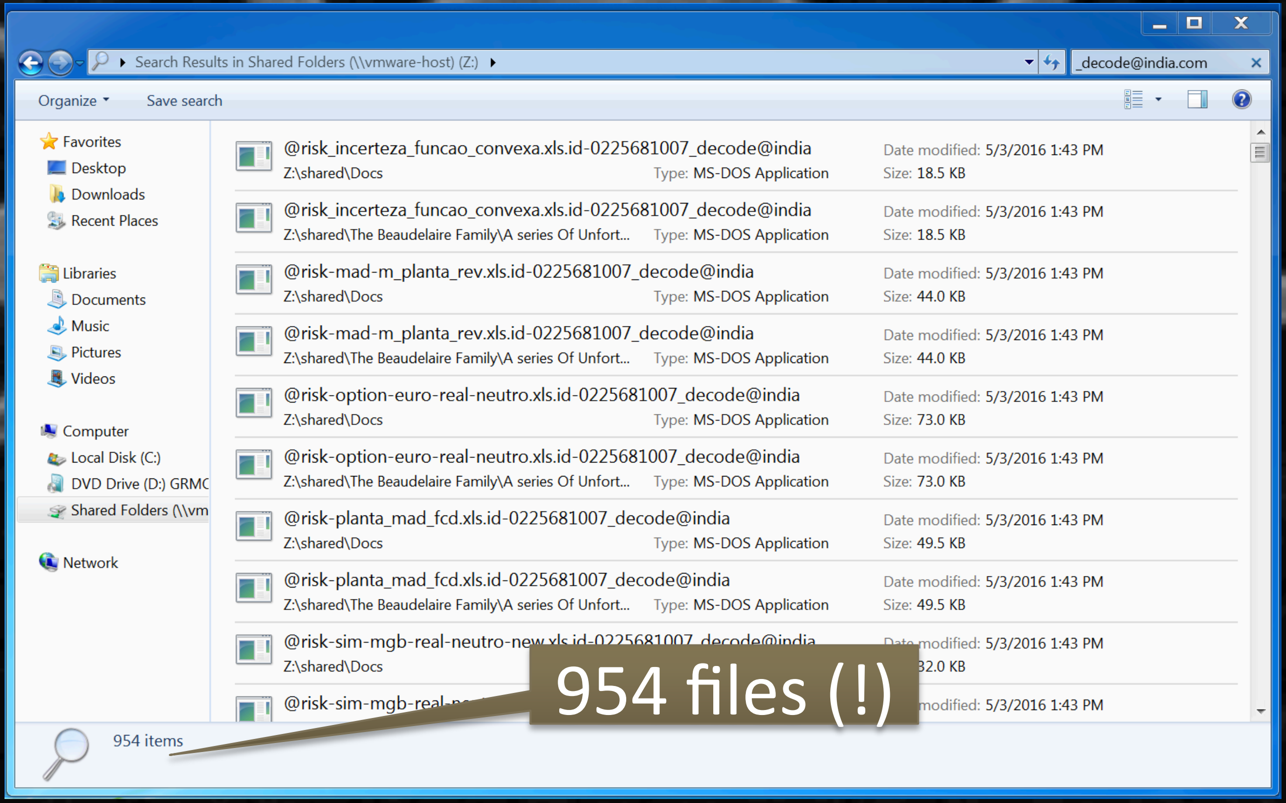


```
05/03/2016  01:43 PM            65,540 simula-mgbs_correlac.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            62,468 simula-real-neutral.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM           297,988 simulation-oligopoly_equilibrium.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM           240,132 simulation-reversion-jumps-marlim-real_x_rn.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            44,548 simulation_reversion-model1.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            12,452 Slangen og den lille Pige_123-1 (24).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            58,500 STATEMENT OF RECEIPT BY STUDENT_120-1 (21).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            87,988 Streaming-Video-From-YouTube.pdf.id-0225681007_decode@india.com
05/03/2016  01:43 PM           231,428 SWLOAD4.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM           246,276 Table 1a.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM           248,836 Table 1b.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            95,236 Table 2a.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            98,820 Table 2b.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            74,756 Table 3a, 3b, 3c.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            35,268 Taller de Seguridad e la_189-1 (90).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            11,188 Tel Fax 27735072775 I am_161-1 (62).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM               964 test.pdf.id-0225681007_decode@india.com
05/03/2016  01:43 PM            99,572 The current status of drug_180-1 (81).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            84,484 time_of_departure.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            81,924 timing-e-97-dif_fin.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            18,436 Tour-de-OC.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            87,044 TourdeSewer.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            49,156 travel_time.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            85,508 UpperBigTujunga.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            16,084 Vereinbarung über die Übermittlungen der_101-1 (2).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM           258,564 war_attrition.xls.id-0225681007_decode@india.com
05/03/2016  01:43 PM            10,708 Waypoints S 33076 32395 13_105-1 (6).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            14,692 Za+é nr 4 Wychowawcy grupy_181-1 (82).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            14,708 Za+é nr 8 Analiza dokumentacji_149-1 (50).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            25,092 Za+é-àcznik 3 Arkusz monitoringu tre+¢ci_141-1 (42).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            16,292 Za+é-àcznik nr 10 Imi-Ö i_164-1 (65).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            22,084 Za+é-àcznik Nr 7 Rozliczenie nauczycieli_152-1 (53).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM           104,660 Zfrtsdavom H4D H5A H90 H00_125-1 (26).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            26,084 µò¦µ+ö µû¦µíê s«ñ TçìFªü µíêS+¦_193-1 (94).docx.id-0225681007_decode@india.com
05/03/2016  01:43 PM            11,012 ßâÉßâÑßâÉßâ¢ßâ¥ßâ¢ßâôßâö ßâÖßâÉßâáßâÿ ßâùßâúßâáßâÑßâùßâÉ ßâ¦ßâÑßâ¥ßâ£ßâôßâÉ ßâ¼ßâÉßâáßâÉßâòßâ
Ùßâÿßâ£ßâ£ßâÉ_134-1 (35).docx.id-0225681007_decode@india.com
             476 File(s)     44,170,944 bytes
The directory name Z:\shared\The Beaudelaire Family\A series Of Unfortunate Events\V                    name\Thi
s is an overly long description of a Projects folder - You see, we are very verbose                     Format f
iles and we also like to be very verbose when making up folder names is too long.

     Total Files Listed:
             924 File(s)     84,419,376 bytes
               0 Dir(s)  251,540,738,048 bytes free

Z:\>
```

924 files

File Explorer

- Find: _decode@india.com



@risk_incerteza_funcao_convexa.xls.id-0225681007_decode@india
Z:\shared\Docs Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 18.5 KB

@risk_incerteza_funcao_convexa.xls.id-0225681007_decode@india
Z:\shared\The Beaudelaire Family\A series Of Unfort... Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 18.5 KB

@risk-mad-m_planta_rev.xls.id-0225681007_decode@india
Z:\shared\Docs Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 44.0 KB

@risk-mad-m_planta_rev.xls.id-0225681007_decode@india
Z:\shared\The Beaudelaire Family\A series Of Unfort... Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 44.0 KB

@risk-option-euro-real-neutro.xls.id-0225681007_decode@india
Z:\shared\Docs Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 73.0 KB

@risk-option-euro-real-neutro.xls.id-0225681007_decode@india
Z:\shared\The Beaudelaire Family\A series Of Unfort... Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 73.0 KB

@risk-planta_mad_fcd.xls.id-0225681007_decode@india
Z:\shared\Docs Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 49.5 KB

@risk-planta_mad_fcd.xls.id-0225681007_decode@india
Z:\shared\The Beaudelaire Family\A series Of Unfort... Type: MS-DOS Application Date modified: 5/3/2016 1:43 PM Size: 49.5 KB

@risk-sim-mgb-real-neutro-new.xls.id-0225681007_decode@india
Z:\shared\Docs Date modified: 5/3/2016 1:43 PM 32.0 KB

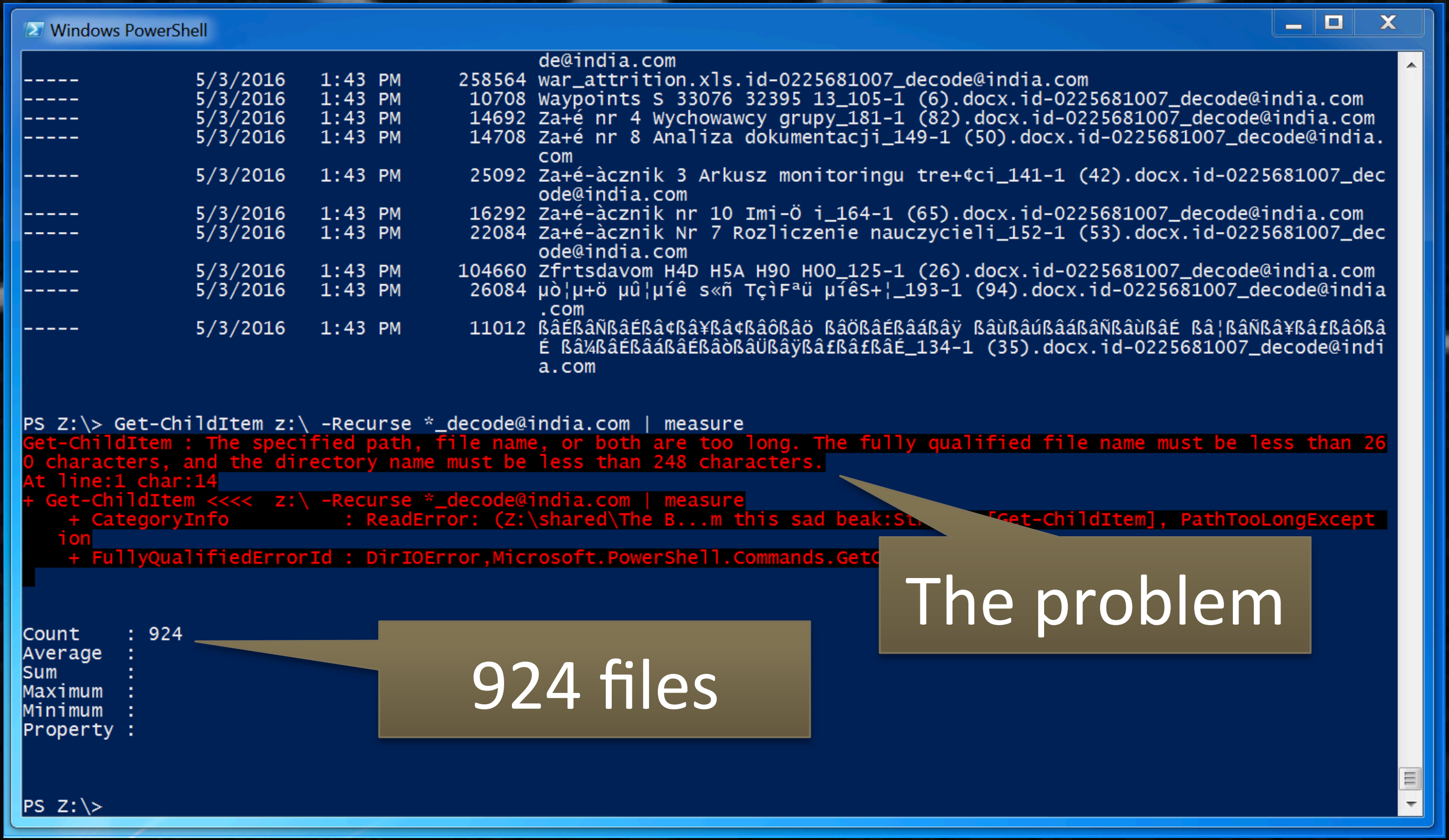
@risk-sim-mgb-real-ne modified: 5/3/2016 1:43 PM

954 items

954 files (!)

Powershell

```
Get-ChildItem Z:\ -Recurse *_decode@india.com
```

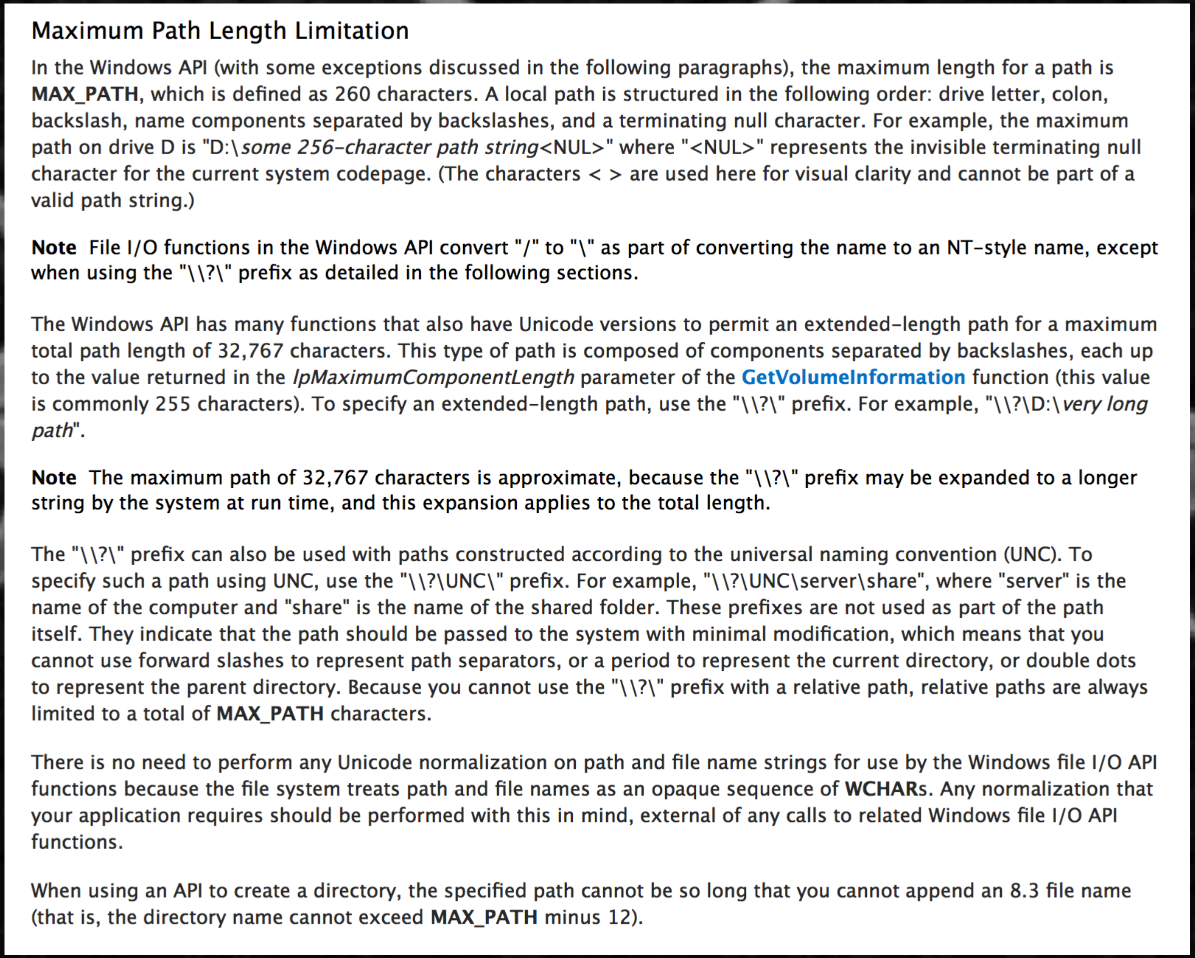


```
                                            de@india.com
-----         5/3/2016   1:43 PM     258564 war_attrition.xls.id-0225681007_decode@india.com
-----         5/3/2016   1:43 PM      10708 Waypoints S 33076 32395 13_105-1 (6).docx.id-0225681007_decode@india.com
-----         5/3/2016   1:43 PM      14692 Za+é nr 4 Wychowawcy grupy_181-1 (82).docx.id-0225681007_decode@india.com
-----         5/3/2016   1:43 PM      14708 Za+é nr 8 Analiza dokumentacji_149-1 (50).docx.id-0225681007_decode@india.
                                            com
-----         5/3/2016   1:43 PM      25092 Za+é-àcznik 3 Arkusz monitoringu tre+¢ci_141-1 (42).docx.id-0225681007_dec
                                            ode@india.com
-----         5/3/2016   1:43 PM      16292 Za+é-àcznik nr 10 Imi-Ö i_164-1 (65).docx.id-0225681007_decode@india.com
-----         5/3/2016   1:43 PM      22084 Za+é-àcznik Nr 7 Rozliczenie nauczycieli_152-1 (53).docx.id-0225681007_dec
                                            ode@india.com
-----         5/3/2016   1:43 PM     104660 Zfrtsdavom H4D H5A H90 H00_125-1 (26).docx.id-0225681007_decode@india.com
-----         5/3/2016   1:43 PM      26084 µò¦µ+ö µû¦µíê s«ñ TçìFªü µíêS+¦_193-1 (94).docx.id-0225681007_decode@india
                                            .com
-----         5/3/2016   1:43 PM      11012 ßâÉßâÑßâÉßâ¢ßâ¥ßâ¢ßâôßâö ßâÖßâÉßâáßâÿ ßâùßâúßâáßâÑßâùßâÉ ßâ¦ßâÑßâ¥ßâ£ßâôßâ
                                            É ßâ¼ßâÉßâáßâÉßâòßâÜßâÿßâ£ßâ£ßâÉ_134-1 (35).docx.id-0225681007_decode@indi
                                            a.com


PS Z:\> Get-ChildItem z:\ -Recurse *_decode@india.com | measure
Get-ChildItem : The specified path, file name, or both are too long. The fully qualified file name must be less than 26
0 characters, and the directory name must be less than 248 characters.
At line:1 char:14
+ Get-ChildItem <<<<  z:\ -Recurse *_decode@india.com | measure
    + CategoryInfo          : ReadError: (Z:\shared\The B...m this sad beak:St      [Get-ChildItem], PathTooLongExcept
   ion
    + FullyQualifiedErrorId : DirIOError,Microsoft.PowerShell.Commands.GetC


Count    : 924
Average  :
Sum      :
Maximum  :
Minimum  :
Property :


PS Z:\>
```

The problem

924 files

Path Length Limitation



Maximum Path Length Limitation

In the Windows API (with some exceptions discussed in the following paragraphs), the maximum length for a path is **MAX_PATH**, which is defined as 260 characters. A local path is structured in the following order: drive letter, colon, backslash, name components separated by backslashes, and a terminating null character. For example, the maximum path on drive D is "D:\some 256-character path string<NUL>" where "<NUL>" represents the invisible terminating null character for the current system codepage. (The characters < > are used here for visual clarity and cannot be part of a valid path string.)

Note File I/O functions in the Windows API convert "/" to "\" as part of converting the name to an NT-style name, except when using the "\\?\" prefix as detailed in the following sections.

The Windows API has many functions that also have Unicode versions to permit an extended-length path for a maximum total path length of 32,767 characters. This type of path is composed of components separated by backslashes, each up to the value returned in the *lpMaximumComponentLength* parameter of the **GetVolumeInformation** function (this value is commonly 255 characters). To specify an extended-length path, use the "\\?\" prefix. For example, "\\?\D:\very long path".

Note The maximum path of 32,767 characters is approximate, because the "\\?\" prefix may be expanded to a longer string by the system at run time, and this expansion applies to the total length.

The "\\?\" prefix can also be used with paths constructed according to the universal naming convention (UNC). To specify such a path using UNC, use the "\\?\UNC\" prefix. For example, "\\?\UNC\server\share", where "server" is the name of the computer and "share" is the name of the shared folder. These prefixes are not used as part of the path itself. They indicate that the path should be passed to the system with minimal modification, which means that you cannot use forward slashes to represent path separators, or a period to represent the current directory, or double dots to represent the parent directory. Because you cannot use the "\\?\" prefix with a relative path, relative paths are always limited to a total of **MAX_PATH** characters.

There is no need to perform any Unicode normalization on path and file name strings for use by the Windows file I/O API functions because the file system treats path and file names as an opaque sequence of **WCHAR**s. Any normalization that your application requires should be performed with this in mind, external of any calls to related Windows file I/O API functions.

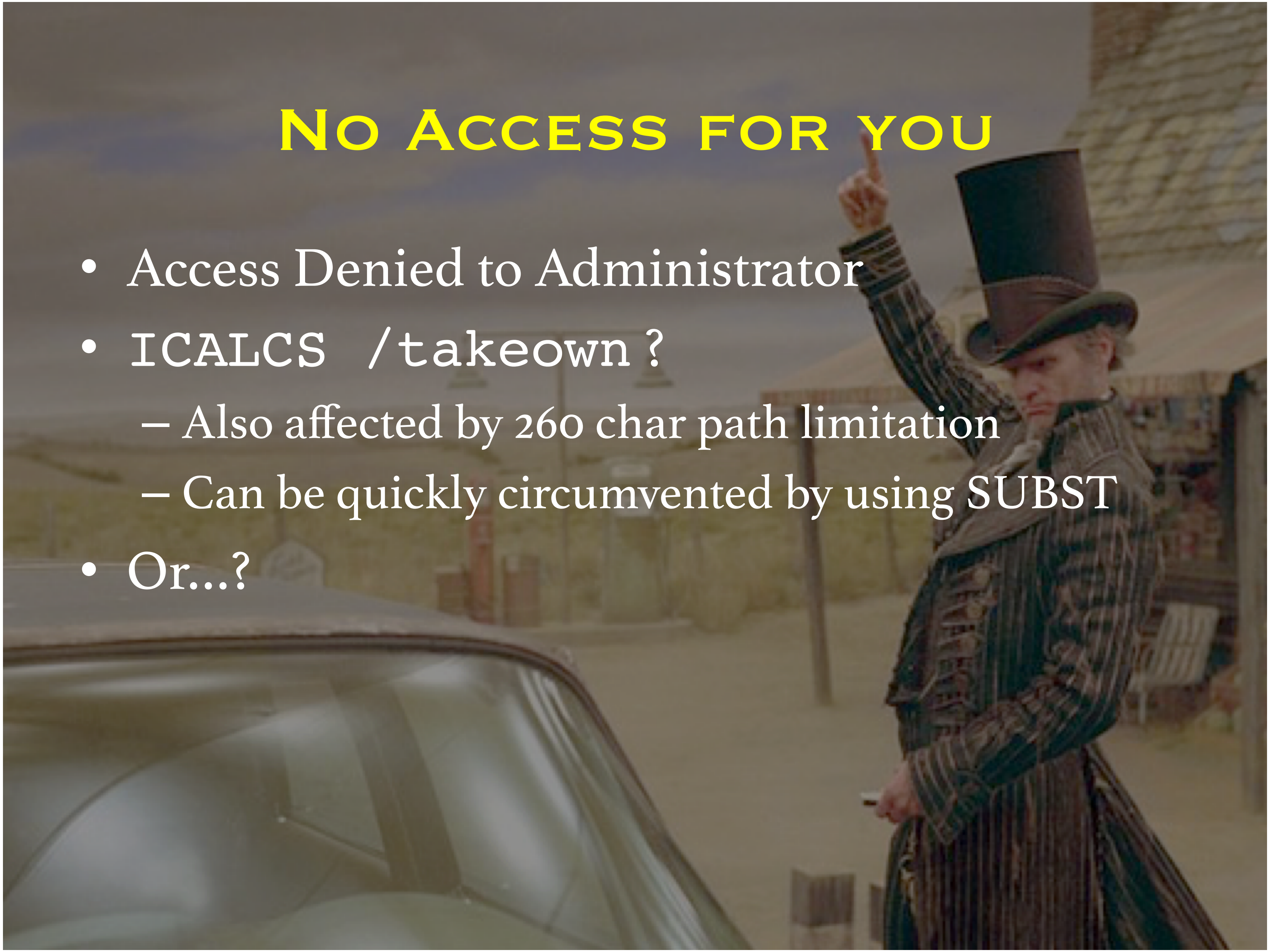
When using an API to create a directory, the specified path cannot be so long that you cannot append an 8.3 file name (that is, the directory name cannot exceed **MAX_PATH** minus 12).

https://msdn.microsoft.com/en-us/library/aa365247.aspx

The Ersatz Elevator

```
SUBST S: "C:\This Is A Very, very, ..., very Long
Folder Name"
DIR /s S:
```

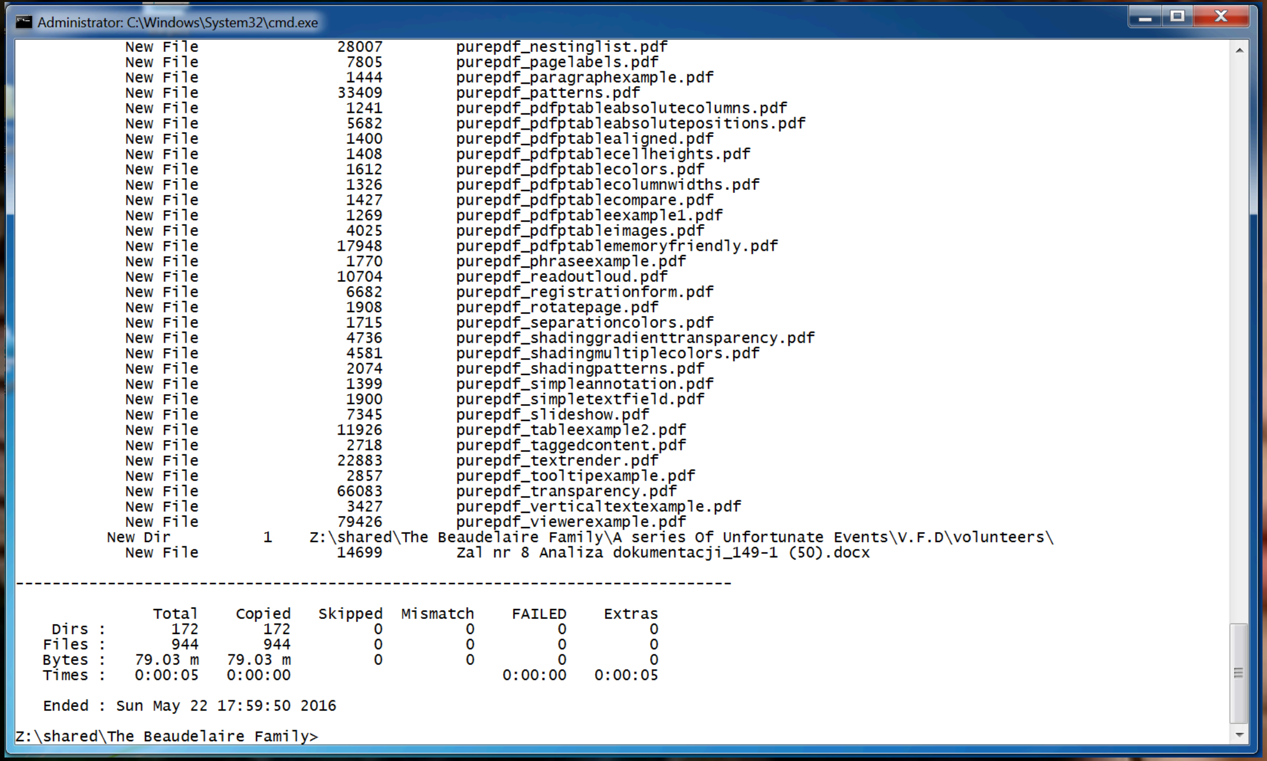
No Access for you



- Access Denied to Administrator
- `ICALCS /takeown`?
  - Also affected by 260 char path limitation
  - Can be quickly circumvented by using SUBST
- Or…?

Robocopy FTW!

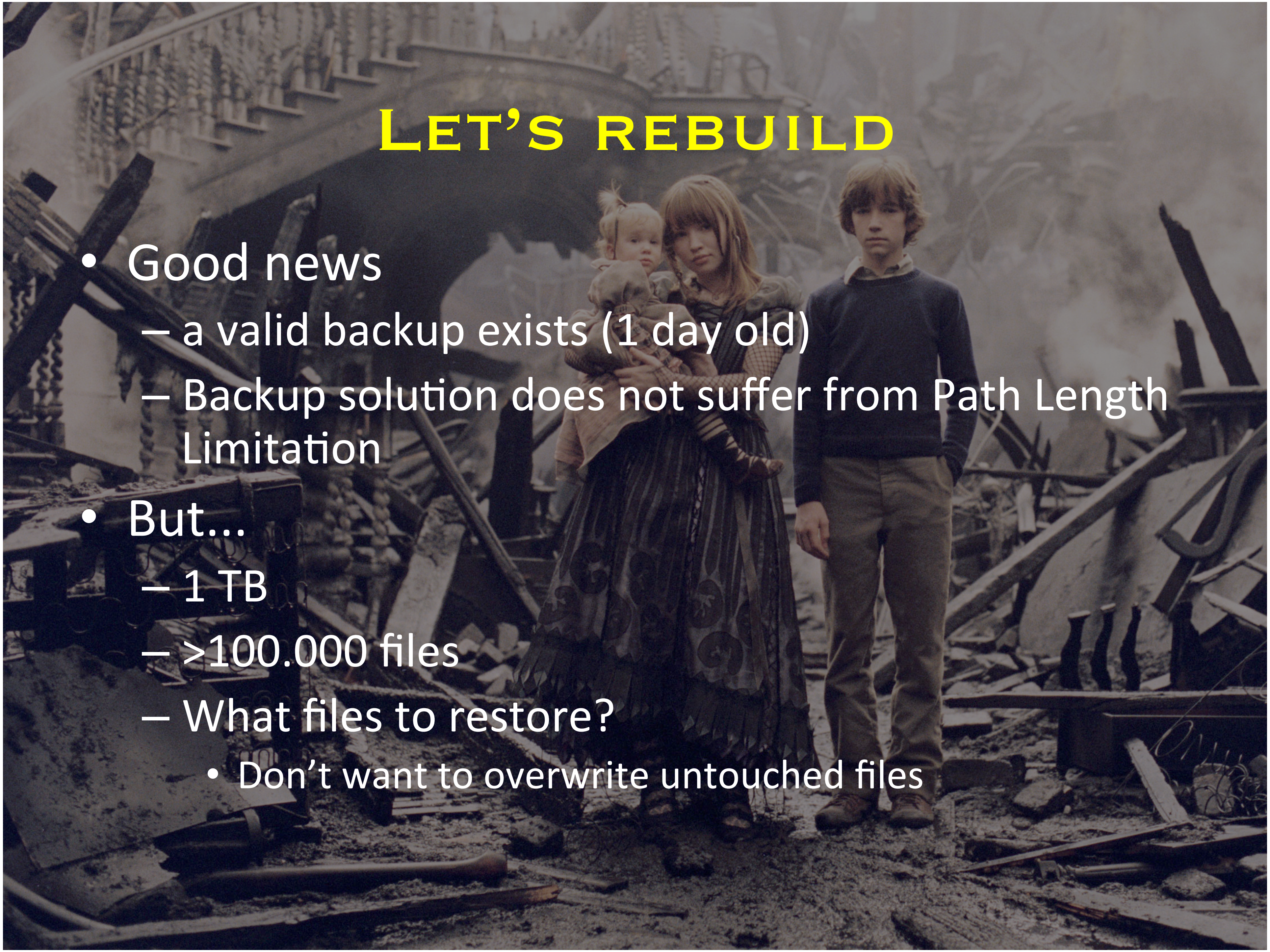
```
ROBOCOPY Z: NULL /E /B /L
```



```
            New File               28007        purepdf_nestinglist.pdf
            New File                7805        purepdf_pagelabels.pdf
            New File                1444        purepdf_paragraphexample.pdf
            New File               33409        purepdf_patterns.pdf
            New File                1241        purepdf_pdfptableabsolutecolumns.pdf
            New File                5682        purepdf_pdfptableabsolutepositions.pdf
            New File                1400        purepdf_pdfptablealigned.pdf
            New File                1408        purepdf_pdfptablecellheights.pdf
            New File                1612        purepdf_pdfptablecolors.pdf
            New File                1326        purepdf_pdfptablecolumnwidths.pdf
            New File                1427        purepdf_pdfptablecompare.pdf
            New File                1269        purepdf_pdfptableexample1.pdf
            New File                4025        purepdf_pdfptableimages.pdf
            New File               17948        purepdf_pdfptablememoryfriendly.pdf
            New File                1770        purepdf_phraseexample.pdf
            New File               10704        purepdf_readoutloud.pdf
            New File                6682        purepdf_registrationform.pdf
            New File                1908        purepdf_rotatepage.pdf
            New File                1715        purepdf_separationcolors.pdf
            New File                4736        purepdf_shadinggradienttransparency.pdf
            New File                4581        purepdf_shadingmultiplecolors.pdf
            New File                2074        purepdf_shadingpatterns.pdf
            New File                1399        purepdf_simpleannotation.pdf
            New File                1900        purepdf_simpletextfield.pdf
            New File                7345        purepdf_slideshow.pdf
            New File               11926        purepdf_tableexample2.pdf
            New File                2718        purepdf_taggedcontent.pdf
            New File               22883        purepdf_textrender.pdf
            New File                2857        purepdf_tooltipexample.pdf
            New File               66083        purepdf_transparency.pdf
            New File                3427        purepdf_verticaltextexample.pdf
            New File               79426        purepdf_viewerexample.pdf
          New Dir          1    Z:\shared\The Beaudelaire Family\A series Of Unfortunate Events\V.F.D\volunteers\
            New File               14699        Zal nr 8 Analiza dokumentacji_149-1 (50).docx

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :       172       172         0         0         0         0
   Files :       944       944         0         0         0         0
   Bytes :   79.03 m   79.03 m         0         0         0         0
   Times :   0:00:05   0:00:00                       0:00:00   0:00:05

   Ended : Sun May 22 17:59:50 2016

Z:\shared\The Beaudelaire Family>
```

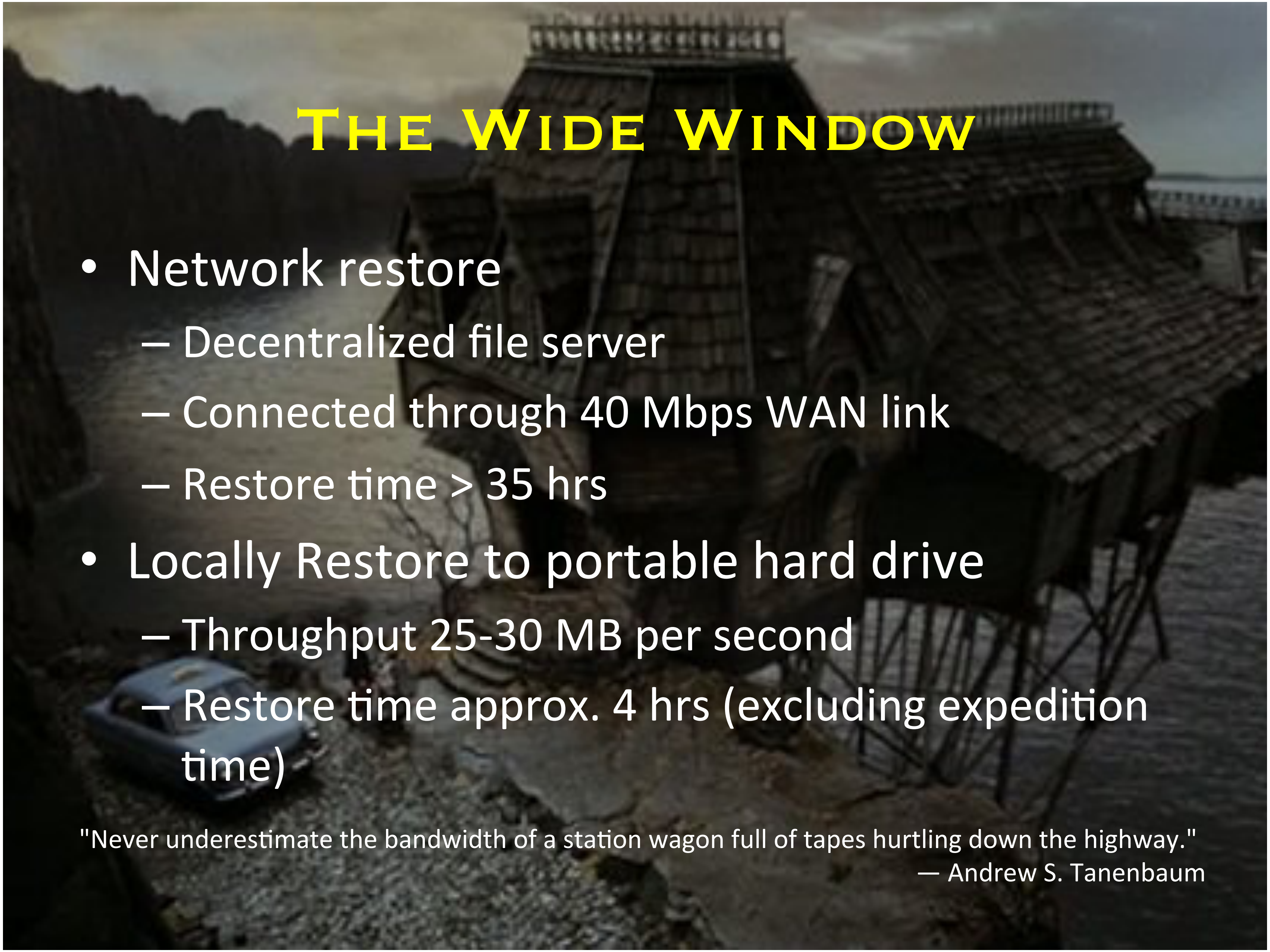
Powershell & Robocopy

- https://learn-powershell.net/2013/04/01/list-all-files-regardless-of-260-character-path-restriction-using-powershell-and-robocopy/



Let’s rebuild

- Good news
  - a valid backup exists (1 day old)
  - Backup solution does not suffer from Path Length Limitation
- But...
  - 1 TB
  - >100.000 files
  - What files to restore?
    - Don’t want to overwrite untouched files



The Wide Window

- Network restore
  - Decentralized file server
  - Connected through 40 Mbps WAN link
  - Restore time > 35 hrs
- Locally Restore to portable hard drive
  - Throughput 25-30 MB per second
  - Restore time approx. 4 hrs (excluding expedition time)

"Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway."
— Andrew S. Tanenbaum

We are done, are we?

Well...

More affected files

- Certain files encrypted but NOT renamed by the ransomware
- How to identify?
  - Filter on Modified timestamp
  - Contains mix of legitimately edited files and malware encrypted files

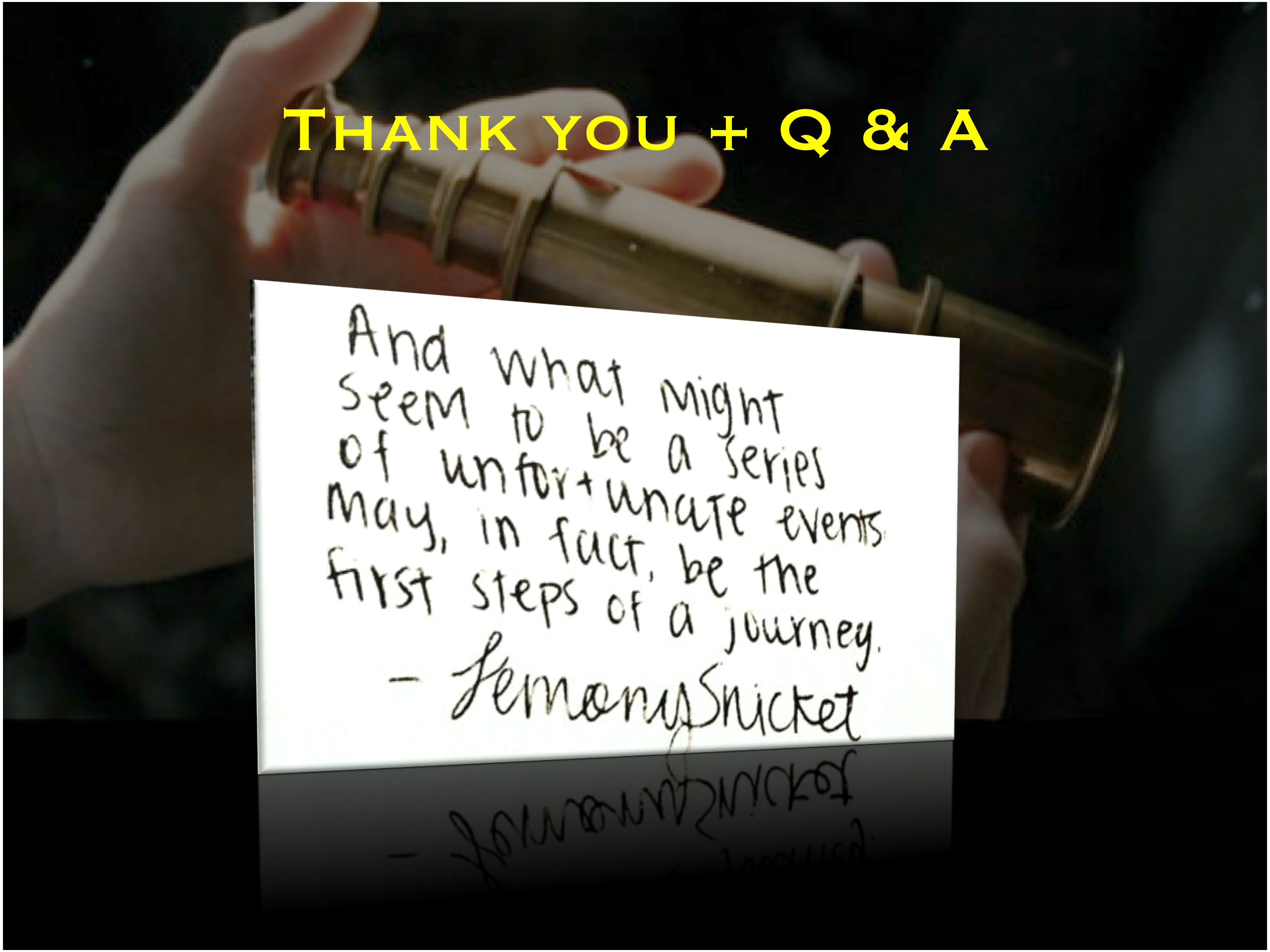
More filtering

- Character Frequency Analysis
  - – High Entropy -> encrypted file!
- Partially encrypted files
  - – High entropy block

Lessons Learned/ Recommendations

- Learn how to identify ransomware species
  - Artifacts, behavior
- Familiarize yourself with non-standard recovery scenario's
  - Can you selectively restore files based on certain criteria?
  - Can you still meet RTO?
- Consider File Share Canaries
- Malware is software and hence is fallible
  - Failure to append file extension
  - Other?
- Backups are key

Thank you + Q & A



And what might seem to be a series of unfortunate events may, in fact, be the first steps of a journey.

– Lemony Snicket

The End