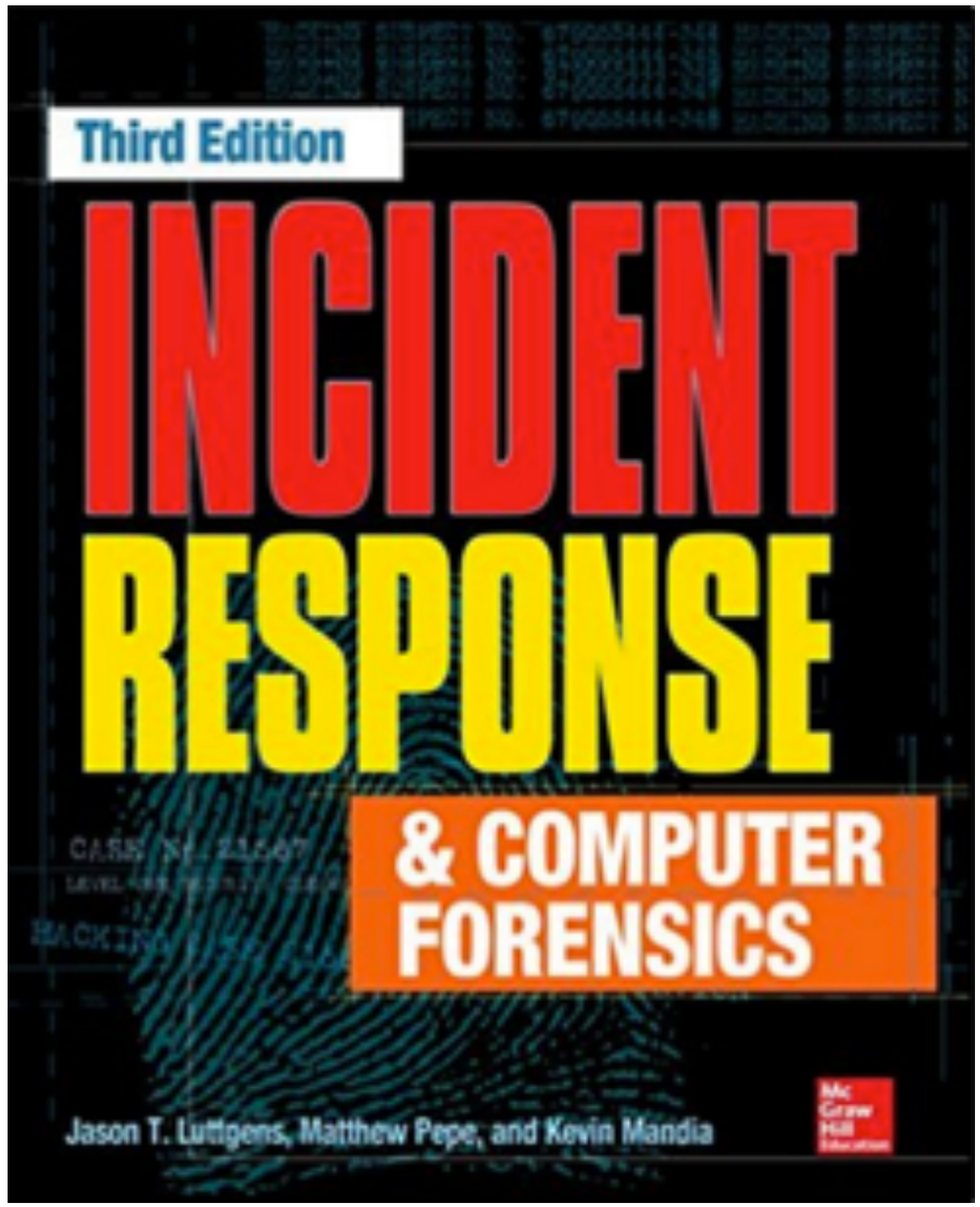
CNIT 152: Incident Response



11 Analysis Methodology

Updated 10-19-22

Process

1. **Define and understand objectives.**
2. **Obtain relevant data.**
3. **Inspect the data content.**
4. **Perform any necessary conversion or normalization.**
5. **Select a method.**
6. **Perform the analysis.**
7. **Evaluate the results.**

Define Objectives

Background

- **You must have a commanding knowledge of both the situation and the technology, understanding:**
  - **What are you looking to determine?**
  - **Is it possible to form a conclusion from the facts you have?**
  - **How long will it take?**

Background

- **What resources will you need?**
- **Who is interested in your results?**
- **What do they plan to do with them?**

Leadership

- **Identify who will define the objectives**
- **Ensure that the entire investigative team knows who that person is**
- **This prevents miscommunication and loss of focus**

Proving a Negative

- **Don't attempt to "prove" that a server was not compromised**
  - **That task is difficult or impossible**
  - **Because you won't have enough information**
  - **Audit trails don't cover every action**
  - **Logs don't go back to the start of time**

Positive Goals

- **Look for a set of indicators of compromise**
- **State if you can find any**
- **If indicators are reasonable,**
  - **You can state an opinion that the system was likely not compromised**
  - **But you don't know for sure**

Realistic Questions

- **Is malware present on this computer?**
  - **Not realistic to determine for sure**
- **Is there an active file with this specific MD5 hash on this computer?**
  - **Realistic, easy to answer**

Scope

- **Too vague:**
  - **Look at this hard drive**
  - **Look at all e-mail**
- **Better:**
  - **Review all active .pst files for any email Bob Smith received within the last month**

Why?

- **Always ask "Why?"**
- **Keep asking questions until the stakeholders come to a consensus about the scope and purpose of the analysis**
- **Analyst may need to define the objectives because the company representatives don't understand what is possible or reasonable**

Know Your Data

Where is Data Stored?

- **Desktop and laptop computers**
- **Hard drives**
- **External storage**
- **Virtual desktops--no local storage, everything on centralized virtualization infrastructure**

Where is Data Stored?

- **Servers**
  - **Data centers, server rooms, or communication closets**
  - **Often rack-mounted**
  - **At least one hard drive for operating system**
  - **May contain additional drives, or use external storage solutions exclusively, especially for virtual servers**

Where is Data Stored?

- **Mobile devices**
  - **Phones, personal digital assistants (PDAs), tablet, wearable computers**
  - **Small amount of nonvolatile storage**
  - **Flash memory**
  - **Expansion slots and ports for external storage devices**

Where is Data Stored?

- **Storage solutions and media**
  - **USB flash drives and hard drives**
  - **CDs and DVDs**
  - **Network Attached Storage (NAS)**
  - **Storage Area Network (SAN)**

Where is Data Stored?

- **Network Devices**
  - **Firewalls, switches, routers**
  - **Typically don't store user data**
  - **Contain configuration and logging data**

Where is Data Stored?

- **Cloud services**
  - **Off-site third-party service hosting data**
  - **Hosted email, timesheets, payroll, human resources**
  - **Dropbox, Google Drive, etc.**

Where is Data Stored?

- **Backups**
  - **Can be stored on local devices**
    - **Disaster recovery plan requires off-site backups**
    - **Most commonly on tape, but could be on USB drives or DVDs**
    - **Cloud-based, like Carbonite or Mozy**

What's Available?

- **Four types of evidence**
  - **Operating system**
  - **Applications**
  - **User data**
  - **Network services and instrumentation**

Operating System

- **File systems like NTFS and HFS+**
- **State information such as running processes and open network ports**
- **OS logs**
- **OS-specific data sources, like Windows registry, Unix syslog, and Apple plist files**

File Systems

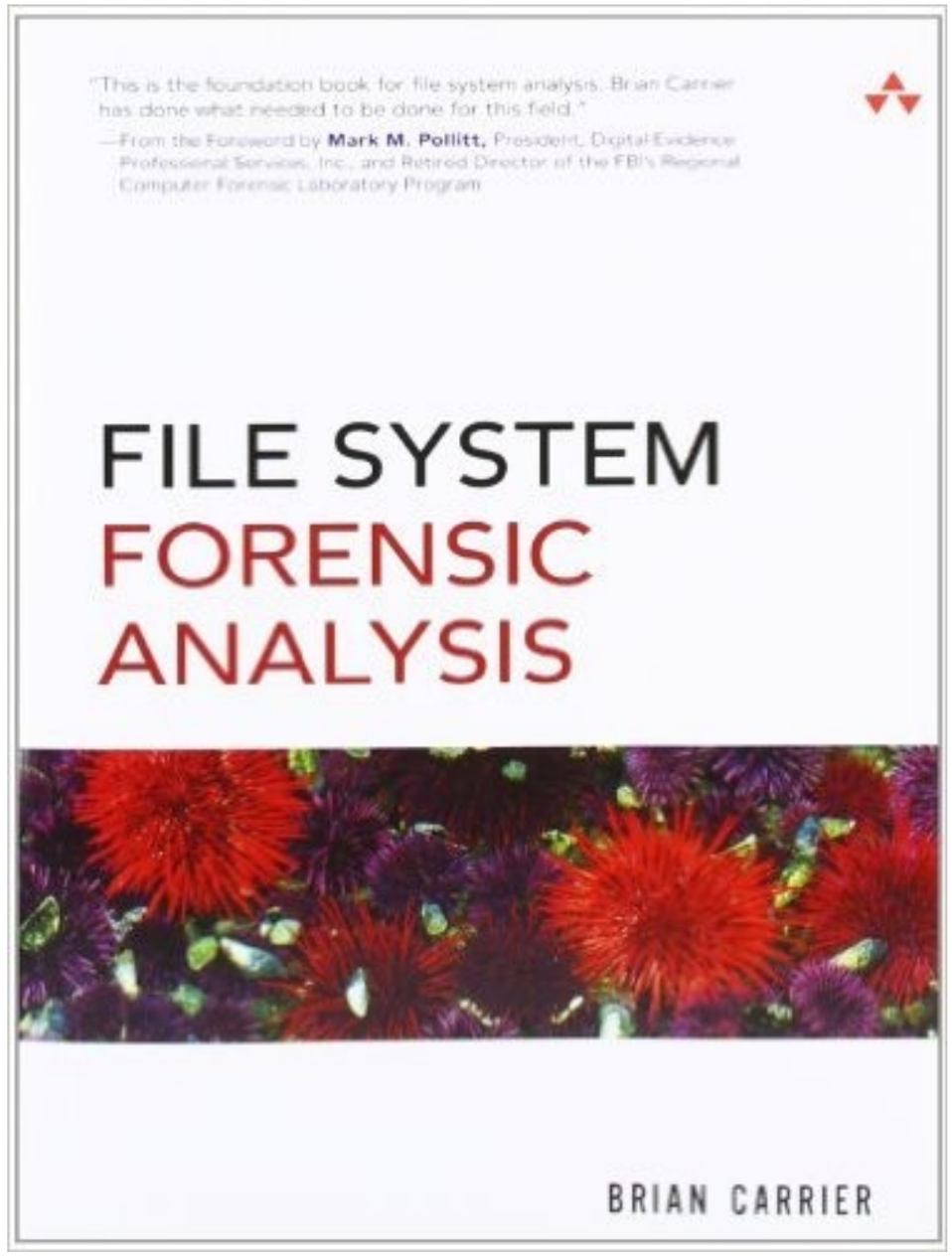
- **Can be independent of operating systems**
- **General concepts:**
  - **Allocation units**
  - **Active files, deleted files**
  - **Timestamps**
  - **Unallocated (free) space, file slack**
  - **Partition tables**

File Systems

- **Unique characteristics, data, and artifacts**
  - **NTFS filename timestamps (link Ch 11i)**
  - **NTFS data streams**
- **UFS inodes**
- **HFS resource forks**
- **File Allocation Table for FAT12, 16, and 32**

Brian Carrier's Book

- **From 2005**
- **Authoritative**
- **Very detailed**
- **Link Ch 11b**



Application-Specific Artifacts

- **Internet browser cache**
- **Database files**
  - **Web server logs**
  - **Chat program user preferences and logs**
  - **Email client data files**
- **Often left behind when applications are uninstalled**

User Data

- **Email, documents, spreadsheets, source code**
- **May be on their day-to-day system**
  - **Or other systems throughout the environment**
- **May be in centralized locations for each user**

Network Services and Instrumentation

- **DHCP, DNS, Proxy servers**
- **Network flow data**
- **IDS/IPS systems**
- **Firewalls**

Access Your Data

Raw Data

- **May be**
  - **Encrypted, compressed, or encoded**
  - **In a custom format**
- **Provided on original hard drives**
- **Contained in hard drive images**
- **Broken**

Ask Questions

- **Determine what you have**
- **If someone else provides the data,**
  - **You must ask good questions**
- **You may have trouble using the data you receive**

Disk Images

- **May be encrypted**
- **Could be logical copy, forensic image, or clone**
- **Could be from a RAID**
- **Three common formats:**
  - **Expert Witness (E01)**
  - **Raw (DD)**
  - **Virtual machine disk files (VMDK, OVF)**

Converting Disk Formats

- **EnCase can handle all three common formats directly**
- **AccessData's FTK Imager can create, convert, and view disk images for many formats**
- **In Linux, you can mount DD images with Filesystem in Userspace (FUSE) and mount E01 images with libewf**

Data Encoding

```
"dGhlIHBhc3N3b3JkIGlzIHNvbHZlY3JpbWU="
":=&AE('!A<W-W;W)D(&ES('-O;'9E8W)I;64`"
"5e0f4784789c4705fa4832aa69d41499"
```

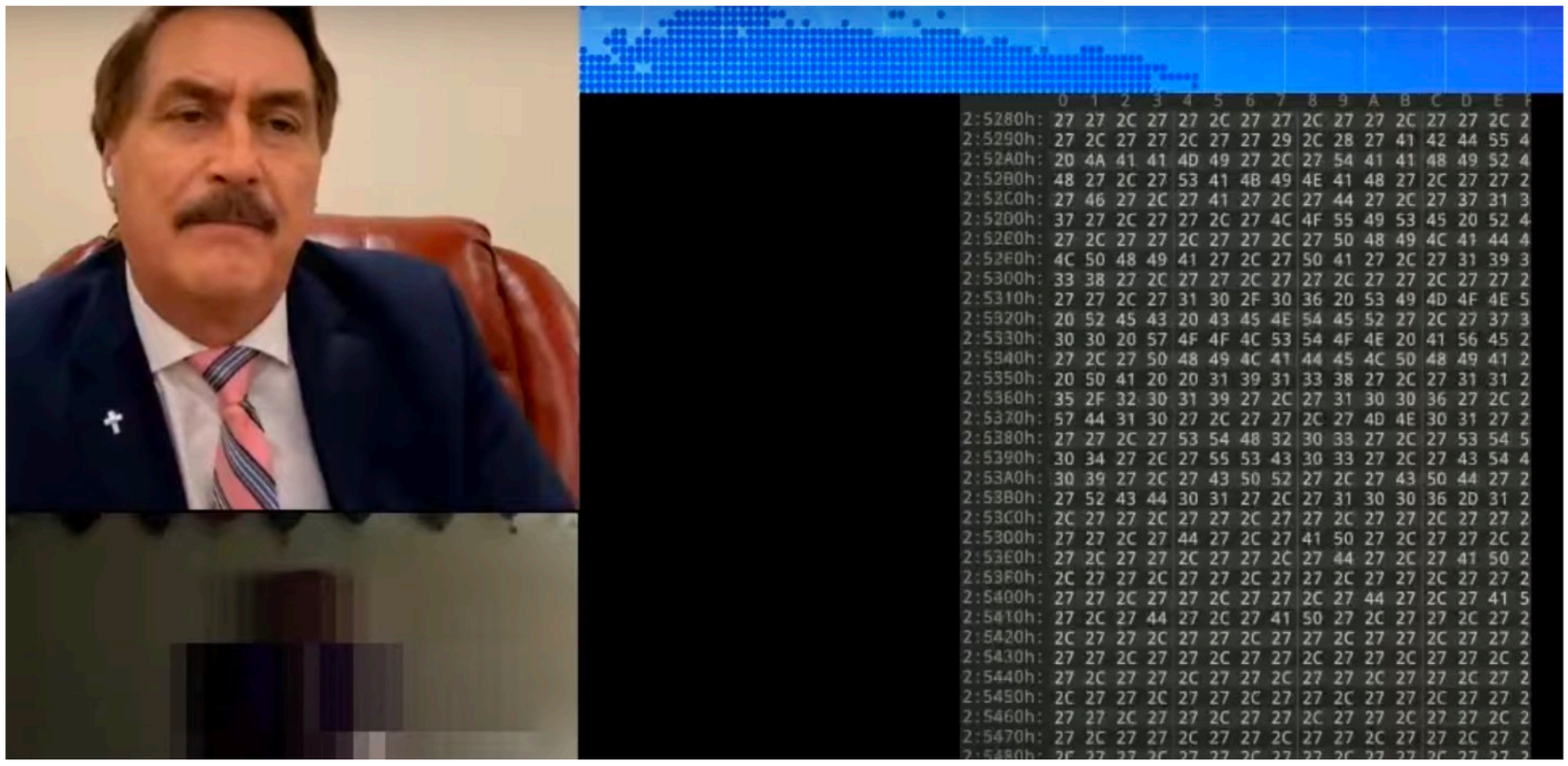
- **All three are "the password is solvecrime" in**
  - **Base64**
  - **UU encoding (link Ch 11k)**
  - **MD5 hash**

Broken Lines

- **This file contains credit card numbers**
- **But a simple text search won't find them because the lines are broken by the hexadecimal values**

```
00000000   54 72 61 6E 73 61 63 74  69 6F 6E 20 62 65 67 69   Transaction begi
00000010   6E 3A 20 32 30 31 33 2D  30 31 2D 30 31 54 30 30   n: 2013-01-01T00
00000020   3A 30 30 3A 30 30 5A 0D  0A 54 72 61 6E 73 61 63   :00:00Z  Transac
00000030   74 69 6F 6E 20 49 44 3A  20 35 34 37 31 32 33 36   tion ID: 5471236
00000040   39 38 35 34 36 35 38 37  0D 0A 43 61 72 64 20 6E   98546587  Card n
00000050   75 6D 62 65 72 3A 20 34  34 34 34 35 35 35 35 36   umber: 444455556
00000060   36 36 36 37 37 37 37 0D  0A 41 6D 6F 75 6E 74 3A   6667777  Amount:
00000070   20 24 31 32 33 2E 34 35  20 55 53 44 0D 0A 2D 2D    $123.45 USD  --
00000080   2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D   ----------------
```

Lindell's "PCAPs"




```
'','','','','','','',''),('[redacted]','[redacted]','[redacted]','''F','A','D','717','','[redacted]
[redacted]','','','PHILADLPHIA','PA','1938','','','','''','10/06 SIMON REC CENTER','700 WOOLSTON AVE','PHILADELPHIA PA
19138','115/2019','103.brWD10','','MN01''','STH203','ST
```

- https://twitter.com/pwnallthethings/status/1400818279292284931

Localizations

- **Different conventions for**
  - **Times, dates, numbers, characters, etc.**
- **Many different formats for dates even at the same location**

Analyze Your Data

Example: Data Theft

- **Start with these types of evidence**
  - **Network anomalies**
  - **Common host-based artifacts of data theft**

Network Anomalies

- **Network flow data**
  - **High outbound volume of data on a single day**
  - **Unusual level of traffic over certain protocols or ports**
- **Proxy logs, DNS logs, firewall logs**
  - **Look for anything suspicious, such as failed login attempts**

Host-Based Artifacts of Data Theft

- **Abnormal user activity**
- **Login activity outside of expected hours**
- **Odd connection durations**
- **Unexpected connection sources (remote session from a workstation to a server, for example)**
- **Periods of abnormally high CPU or disk utilization (common when compressing data)**
- **File artifacts associated with the use of common compression tools**
- **Recently installed or modified services, or the presence of other persistence mechanisms**

Look for Malware

- **Follow the initial leads. For example, if a date is relevant, review system activity for that day. If you know that specific file names are involved, search for them.**
- **Review programs that automatically start.**
- **Verify the integrity of system binaries.**
- **Make a list of and look for other well-known artifacts of an infection.**
- **Perform a virus scan of the system.**

Legitimate Tools

- **LOLBINs "Living off the land"**
- **cmd.exe in a folder other than \Windows\System32 is suspicious**
- **Many compromises use normal system tools, not malware**

Plan Tasks

- **Example: search for abnormal user login times**
  - **Do you already have a way to automate that process?**
    - **You may need to develop a technique, or perform steps manually**
- **Consider volume of data, time required to process, who is available to work on it, and how likely the data source is to answer your question**

Select Methods

- **General methods**
  - **Use of external resources**
  - **Manual inspection**
  - **Use of specialized tools**
  - **Data minimization through sorting and filtering**
  - **Statistical analysis**
  - **Keyword searching**
  - **File and record carving**

External Resources

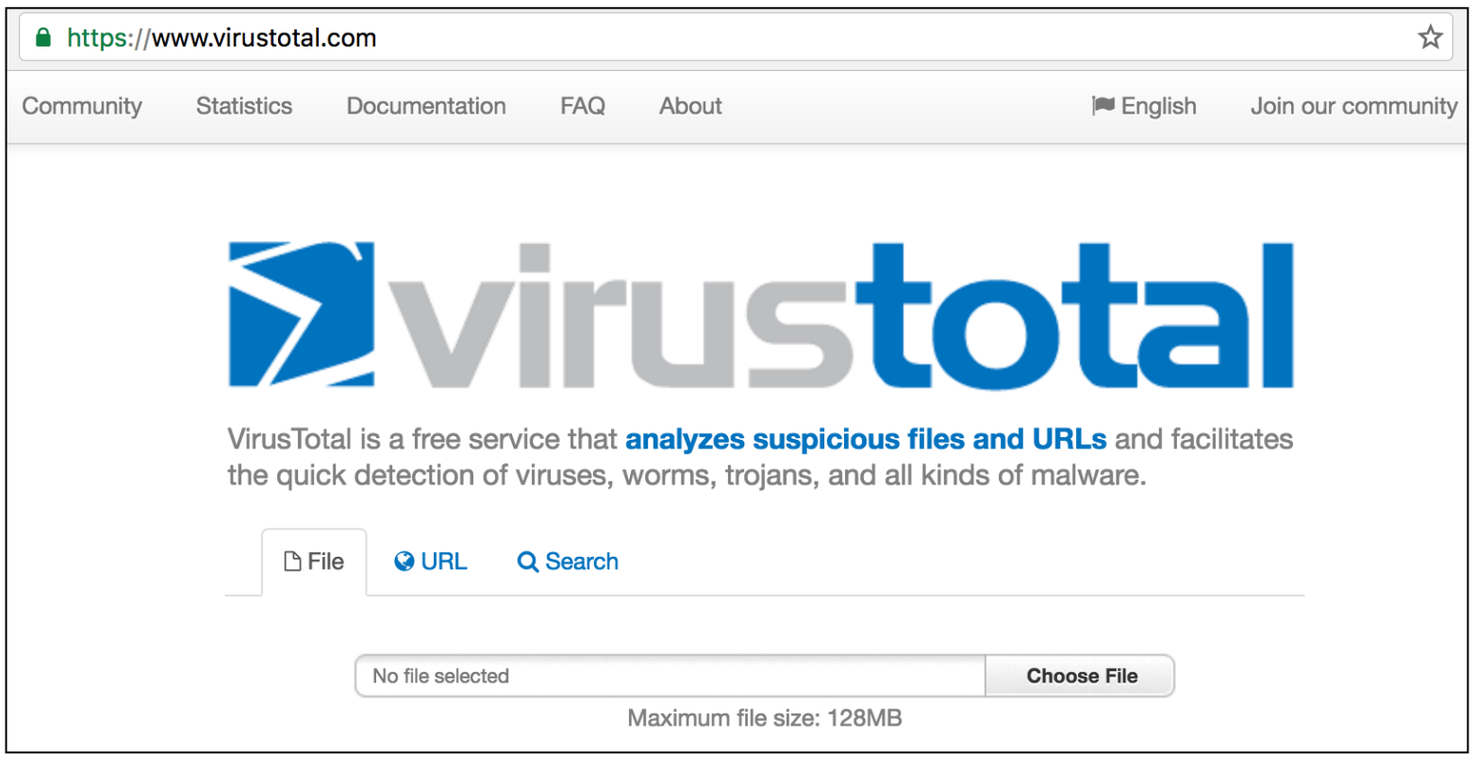
- **Contains MD5 and SHA1 hashes of known files**
- **Exclude known harmless files from analysis**

```
C:\YOURNAME>md5 *.* | nsrllookup.exe -k
74F26FC01B180D4A99A168ED69C30A53  cmd.exe
DAF60E13E96ECB67F0EDAA89C6B01B8D  notepad.exe

C:\YOURNAME>md5 *.* | nsrllookup.exe -u
8D443F2E93A3F0B67F442E4F1D5A4D6D  md5.exe
4AF3F465E8C0FF6B491CC8AE5D105AE2  nsrllookup.exe
```

VirusTotal

- **The standard to test suspicious files**
- **Links to many virus databases**
- **Can work with files or hashes**



VirusTotal Demo

- 1bb93d8cc7440ca2ccc10672347626fa9c3f227f46ca9d1903dd360d9264cb47
  - Behavior, Microsoft Sysinternals, svchost in strange folder, Run keys
    - https://blog.virustotal.com/2021/10/virustotal-multisandbox-microsoft.html

Files Dropped

\+ %USERPROFILE%\AppData\Local\Temp\svchost.exe

Registry Keys Set

\+ HKU\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\1dcc806104fd396681319b614d8b18b5

\+ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\1dcc806104fd396681319b614d8b18b5

VirusTotal Demo

- 1247bb4e1d0aa5aec6fadccaac6e898980ac33b16b69a4aa48fc6e2fb570141d
  - Behavior, Microsoft Sysinternals, Files Dropped, Email
    - https://blog.virustotal.com/2021/10/virustotal-multisandbox-microsoft.html

Files Dropped

+ %USERPROFILE%\AppData\Local\PeerDistRepub
+ %USERPROFILE%\AppData\Local\1247bb4e1d0aa5aec6fadccaac6e898980ac33b16b69a4aa48fc6e2fb570141d.exe
+ %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1247bb4e1d0aa5aec6fadccaac6e898980ac33b16b69a4aa48fc6e2fb570141d
+ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\1247bb4e1d0aa5aec6fadccaac6e898980ac33b16b69a4aa48fc6e2fb570141d.exe
+ C:\$Recycle.Bin\S-1-5-18\desktop.ini.id[584D2235-2275].[raynorzlol@tutanota.com].Adame

Manual Review

- **Small items such as floppy disks can be searched in their entirety manually**
- **Sometimes it's faster to just search manually than to figure out a shortcut**
- **Manual review is also good to validate the results obtained from other methods**
- **Select important samples to review**

Don't Trust Tools Too Much

- **There are many tools that help forensics**
  - **Data visualization**
  - **Browser artifact analysis**
  - **Malware identification**
  - **File system metadata reporting**
- **ALWAYS VERIFY IMPORTANT FINDINGS**
  - **Manually, or with a second tool**
  - **Every tool has bugs**

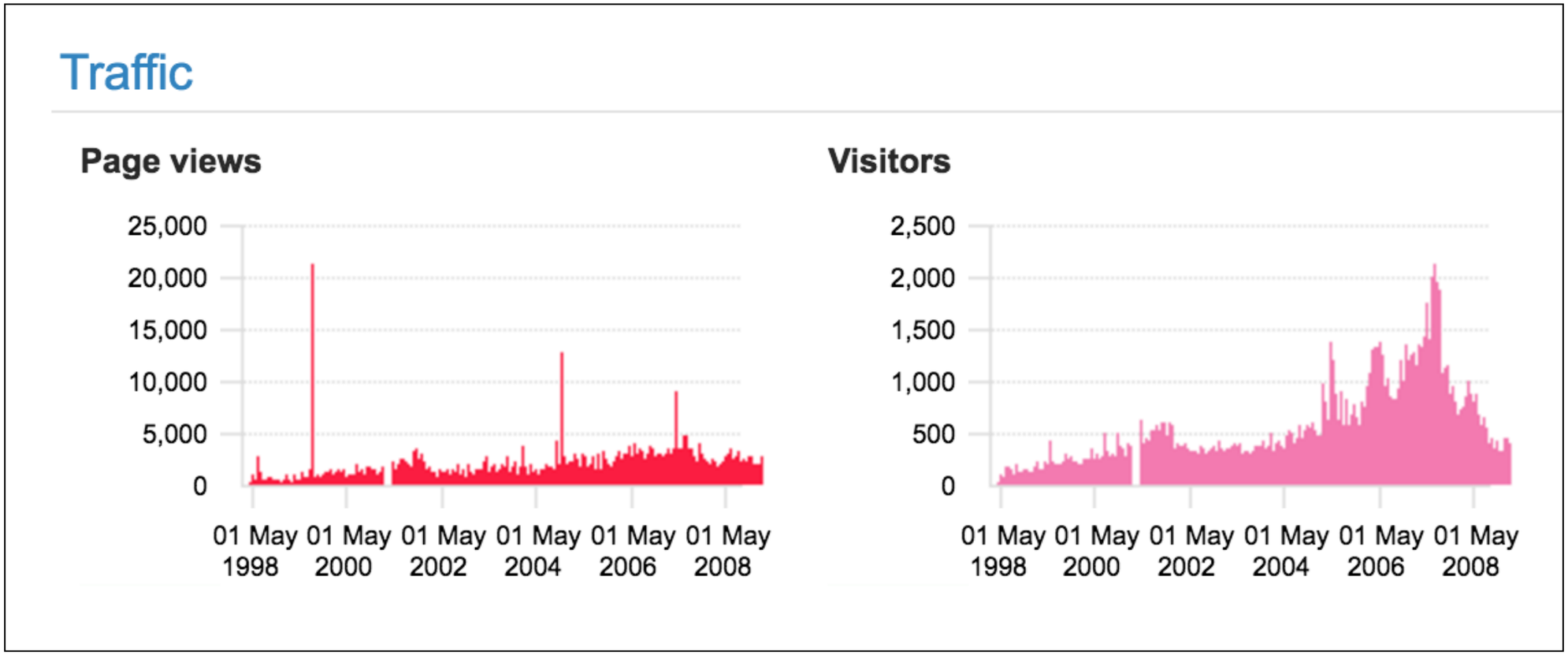
Data Minimization: Sorting & Filtering

- **File system metadata may have hundreds or thousands of files**
- **Need to exclude irrelevant data & focus on the important data**
- **Sort and filter by**
  - **Date, filename, other attributes**

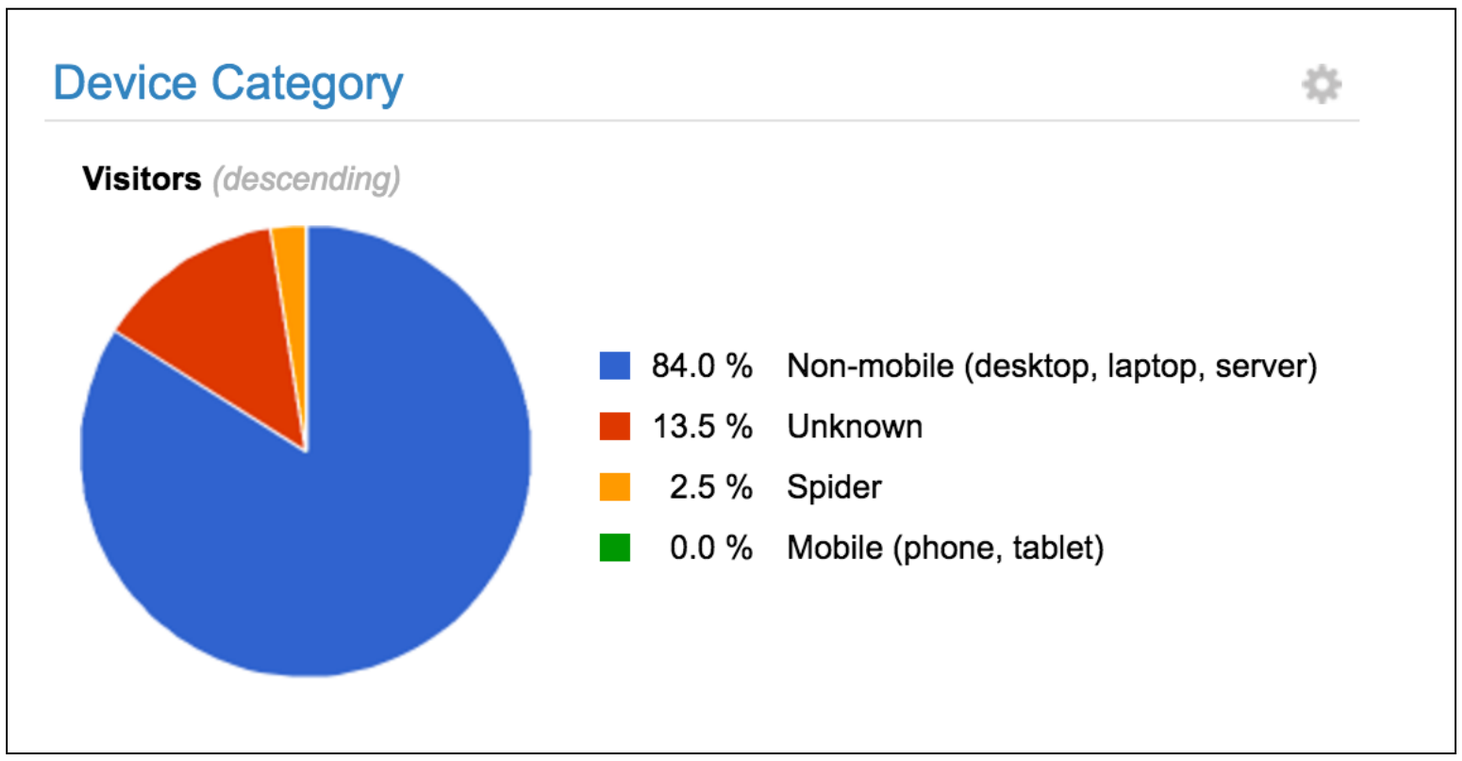
Statistical Analysis

- **You don't know exactly what you are looking for**
  - **Or how to find it**
- **Use statistical analysis to uncover patterns or anomalies**
  - **Ex: Web server logs**
- **Use a log analysis tool to parse data**

Sawmill



- **Link Ch 11a**



String or Keyword Search

- **Create a list of strings relevant to the case**
- **Search the files for those strings**
  - **Emails, Word documents, etc.**
- **Find more strings in those files and repeat**
- **You're done when you aren't finding any new strings to search for**

Unallocated and Slack Space

- **Unallocated blocks often contain portions of deleted files**
- **Unused bytes at the end of active files may also contain fragments of old files**
- **They can both be searched by forensic suites like EnCase, FTK, and Autopsy**

File Carving

- **Look for file headers and footers in unallocated space**
  - **Or other raw data, such as a drive image**
- **Attempt to reconstruct files**
  - **Usually by just taking all data from the header to the footer**
- **Foremost is a good file-carving tool**

Evaluate Results

When to Evaluate Results

- **Periodically throughout the analysis process**
  - **Are you making real progress, or wasting time on a blind alley?**
- **At the end**
  - **How well has your analysis answered the investigative questions?**

Ch 11