Data Hiding Techniques

You can run, but you can't hide for ever…

2014/2015

Dr. Ali Hadi

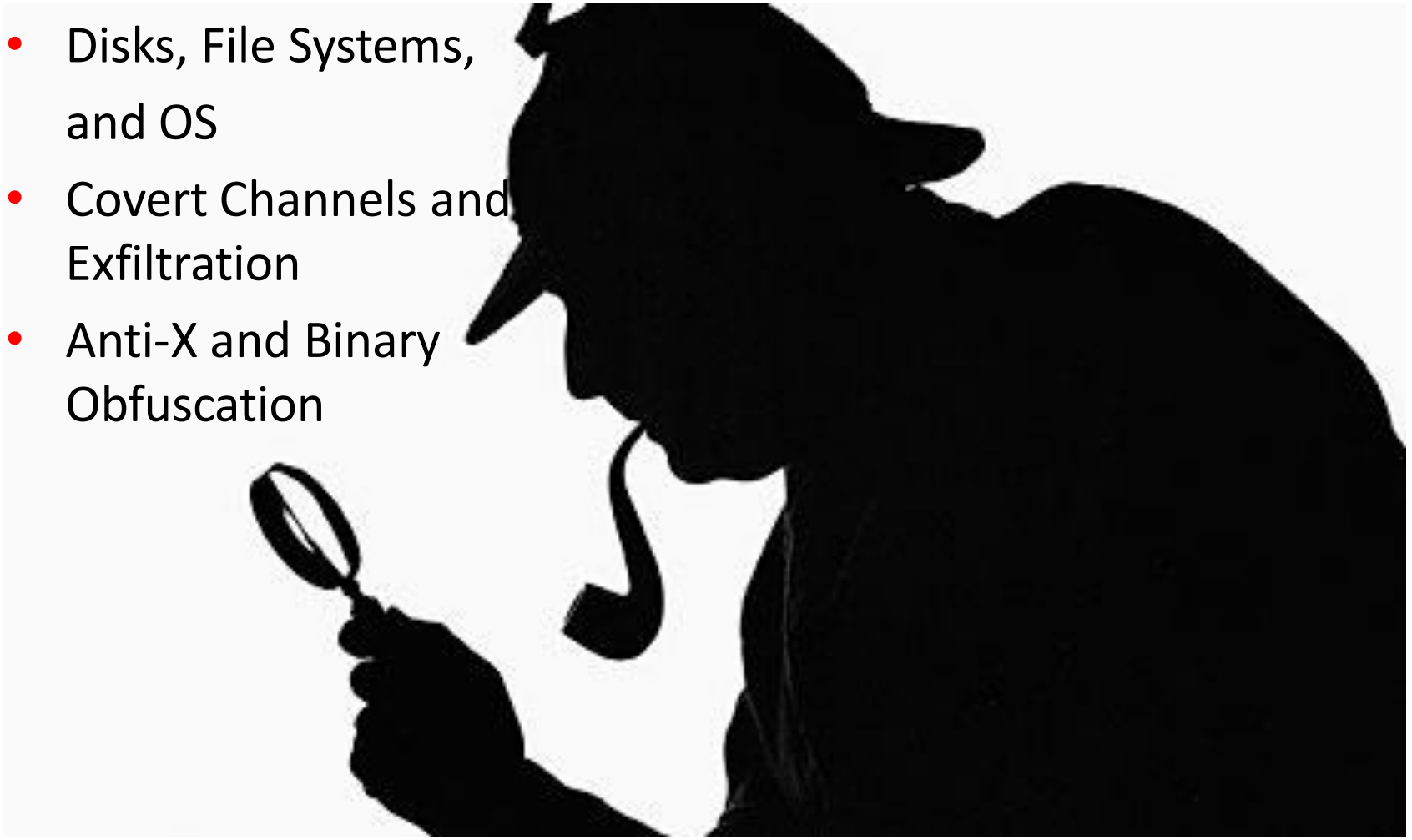
ali@ashemery.com

whoami

- University professor @PSUT by day, DFIR researcher by night!
- PhD research was in “Network Security”
- 14+ years of Professional Experience
- Hold 14+ world known certificate
- Participate in worldwide DFIR challenges
  - Beat participants from top US Corporate, Government, and Law Enforcement Groups
- ***Hacking Techniques and Intrusion Detection*** course published **@OpenSecurityTraining** under the CC license
- Research interests: DFIR, Network and Malware Forensic Analysis, Social Engineering

Outline

- Disks, File Systems, and OS
- Covert Channels and Exfiltration
- Anti-X and Binary Obfuscation

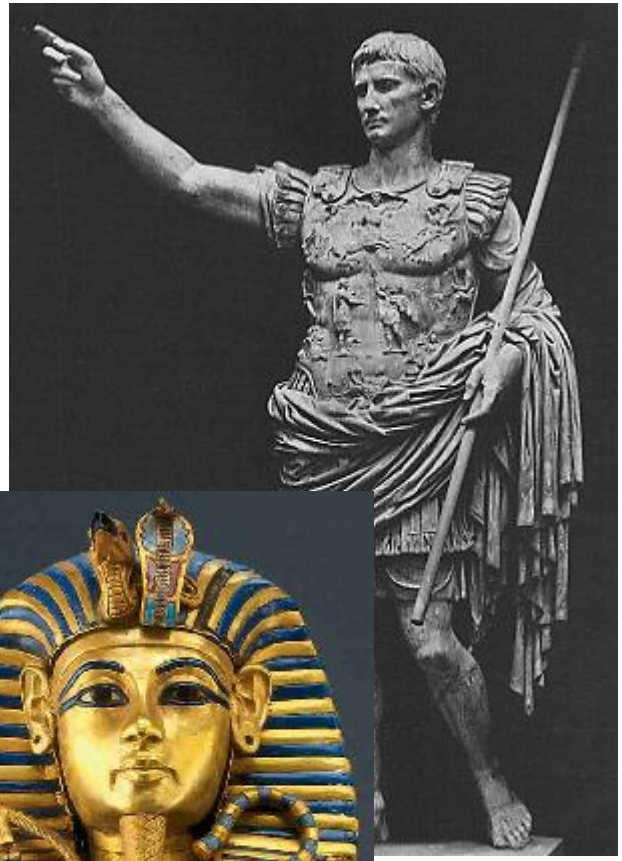


Intro.

"You need to see differently, the sky is not blue any more!"

What?

- Ancient Art
  - Egyptians, Julius Cesar, etc
- Preventing data from being seen
- Good and Evil
- Covert Communication (Secret writing)
- The way used has evolved just as technology has



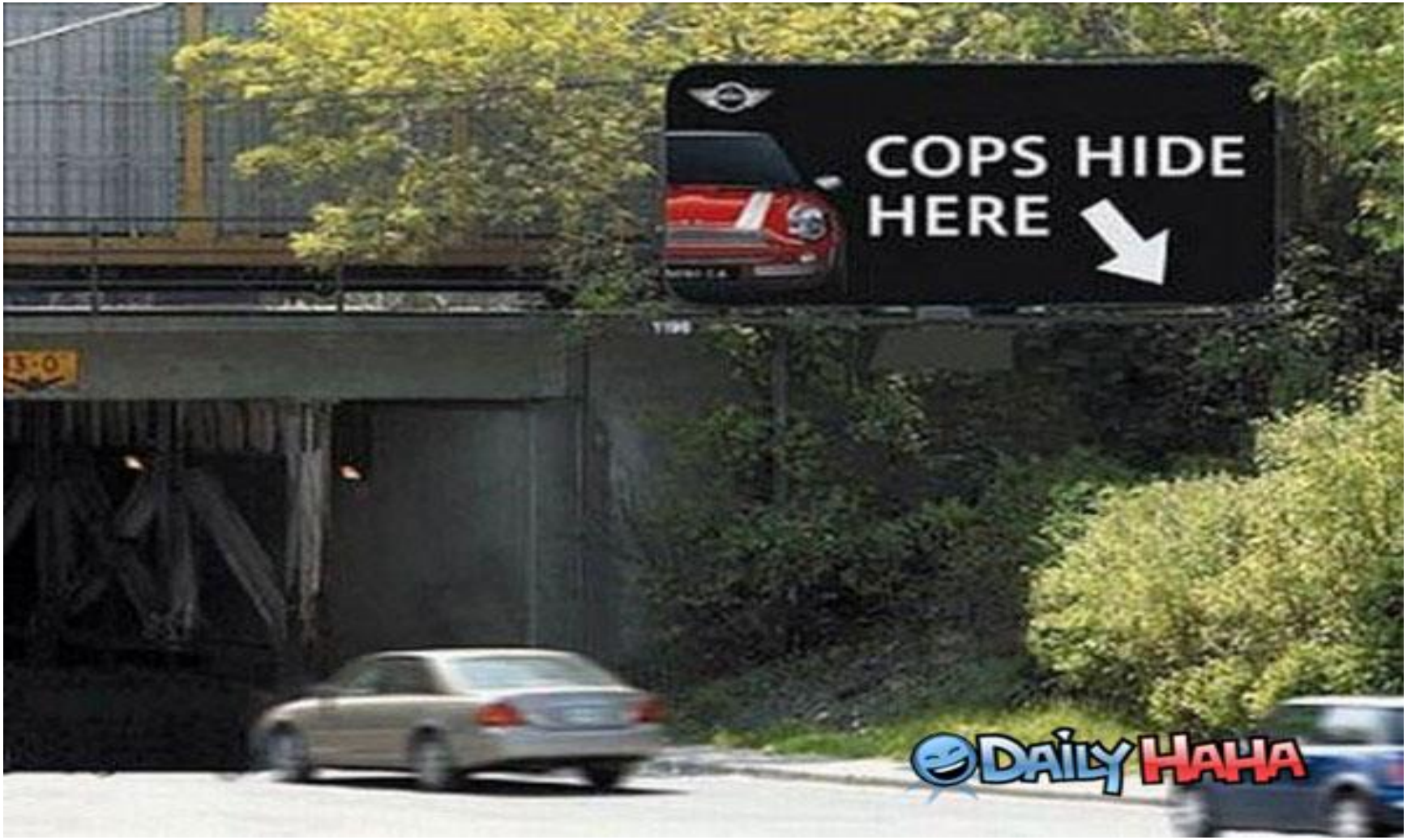
Why?

- Hiding Evidence
- Privacy Issues
- Obfuscating
- Evade Detection (bypassing)
- Exfiltration
  - Espionage
- Data Destruction (deletion or corruption)
- Military
- FUN ☺

Its Not Just ...

- Cryptography
  - Obscuring data into unreadable data
- Steganography
  - Hiding the existence of the data
- Watermarking
  - Proving ownership by adding sufficient metadata

“Data Hiding” in Action

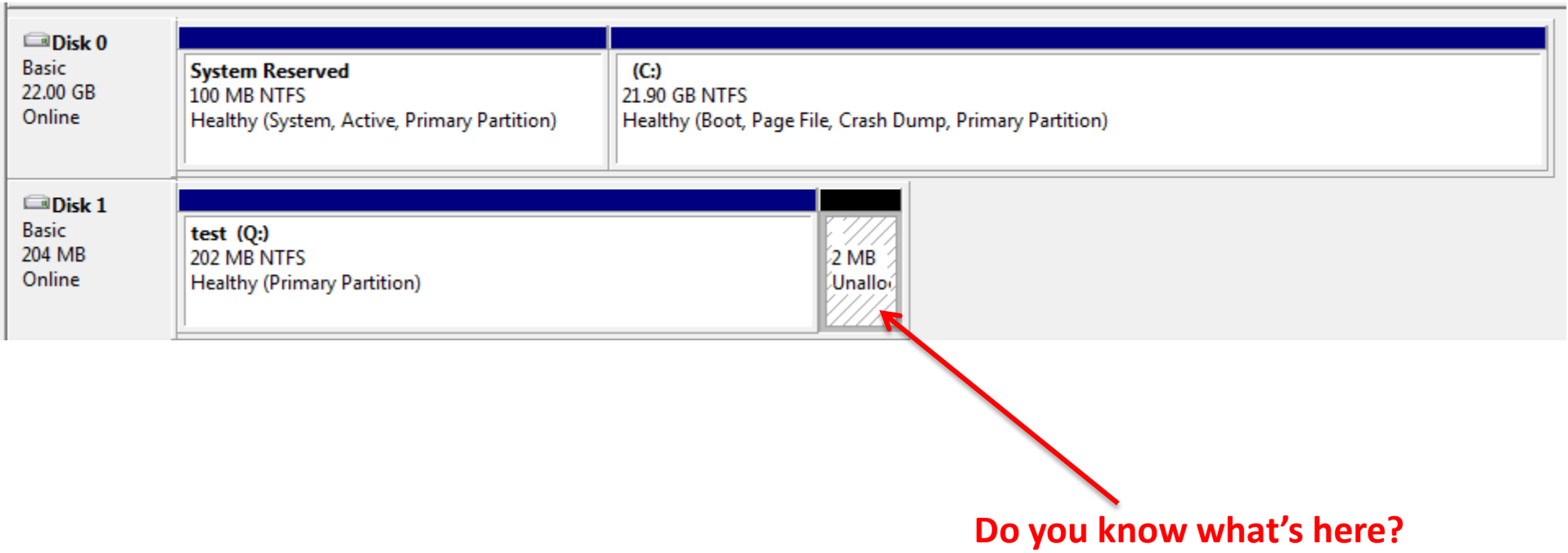


Disks, File Systems, and OS

"Don't be conned by misleading menu structures!"

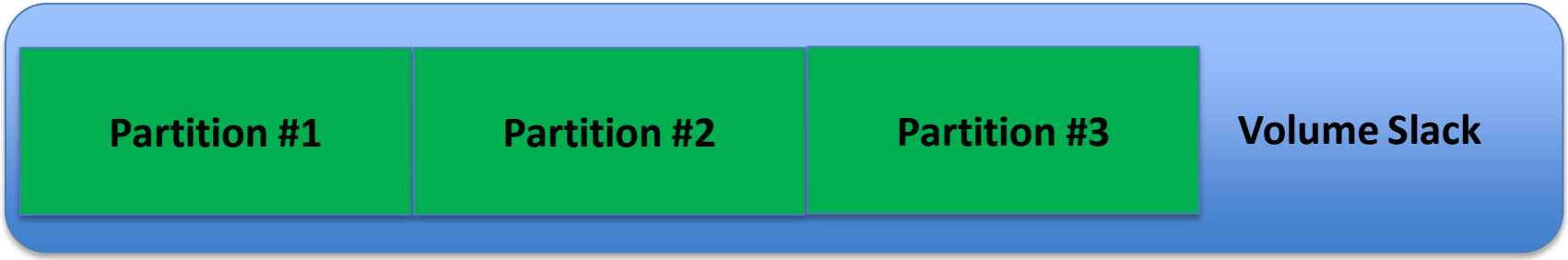
Disks

- Without understanding of disks layout, you'll never know what truly is hidden over there!



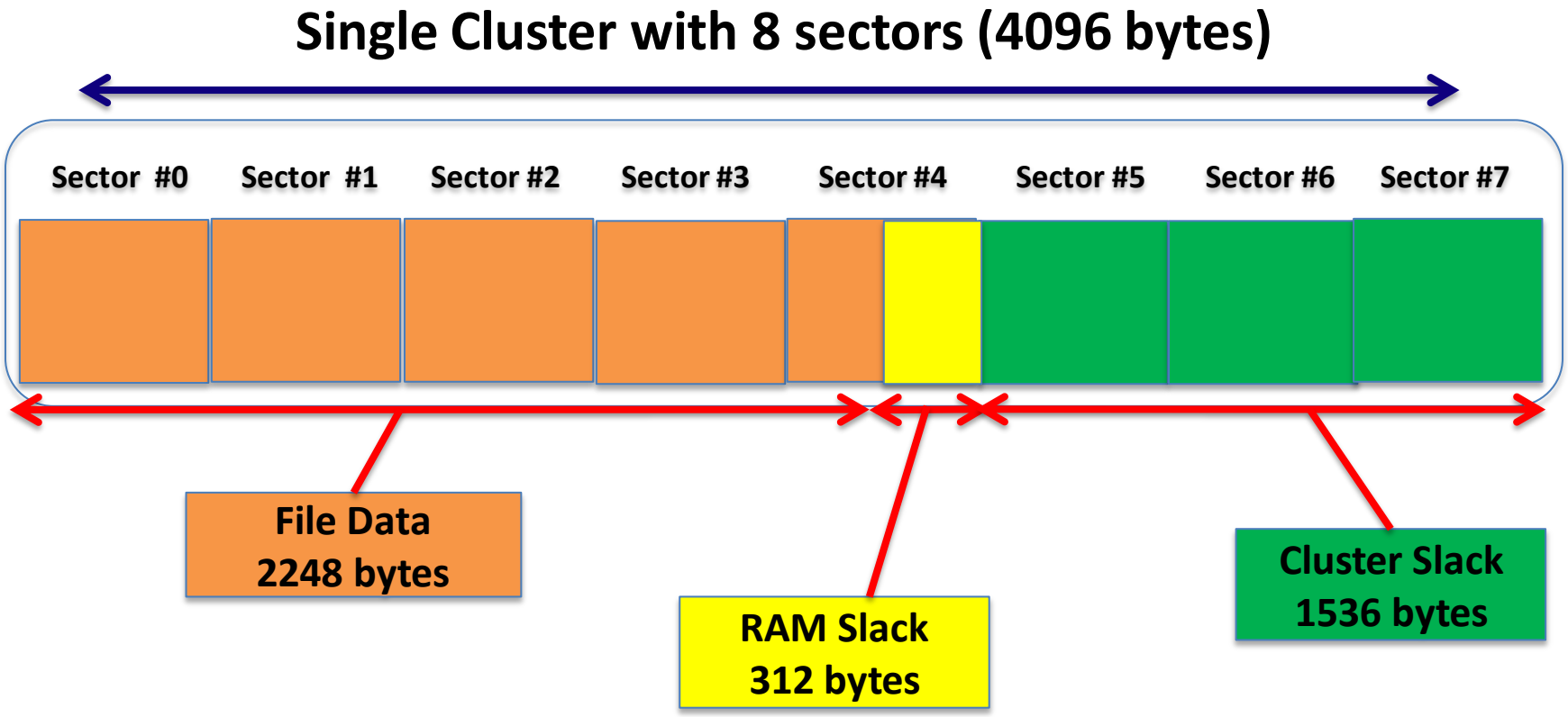
Volume Slack

- Unused space between the end of the volume and the end of the partition
- Size of the hidden data in volume slack is only limited by the space on the hard disk available for a partition



File Slack Space

- Slack space could be used to hide data



File Systems (NTFS)

- Everything written to the disk is considered a **file**
  - Files, directories, metadata, etc

- MFT is the heart of NTFS (array of records 1024 bytes each)
- Records in the MFT are called **metadata**
- First 16 records in the MFT reserved for metadata files
- Entry #1 is **$MFT**

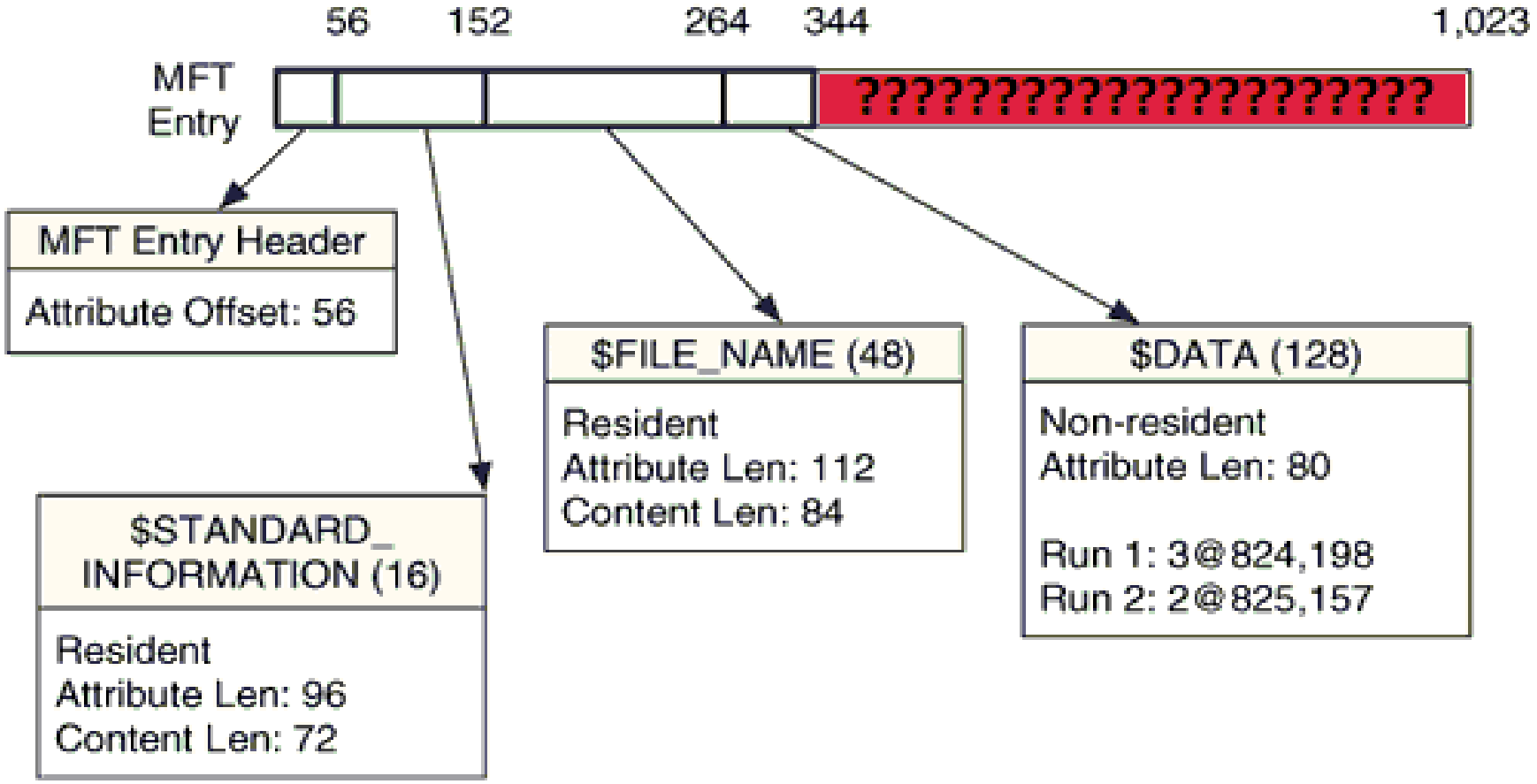
One of the most complex file systems you'll deal with!

File Systems (NTFS) – Cont.

- Deleted Files
  - Unallocated space
  - File System Journals, Index Files, and Log files: **$I30**, **$LogFile**
- File Wippers
  - They don’t actually wipe everything, some crumbs left for investigator!
- Hiding within **$DATA** attribute

MFT Slack Space

- MFT Slack Space



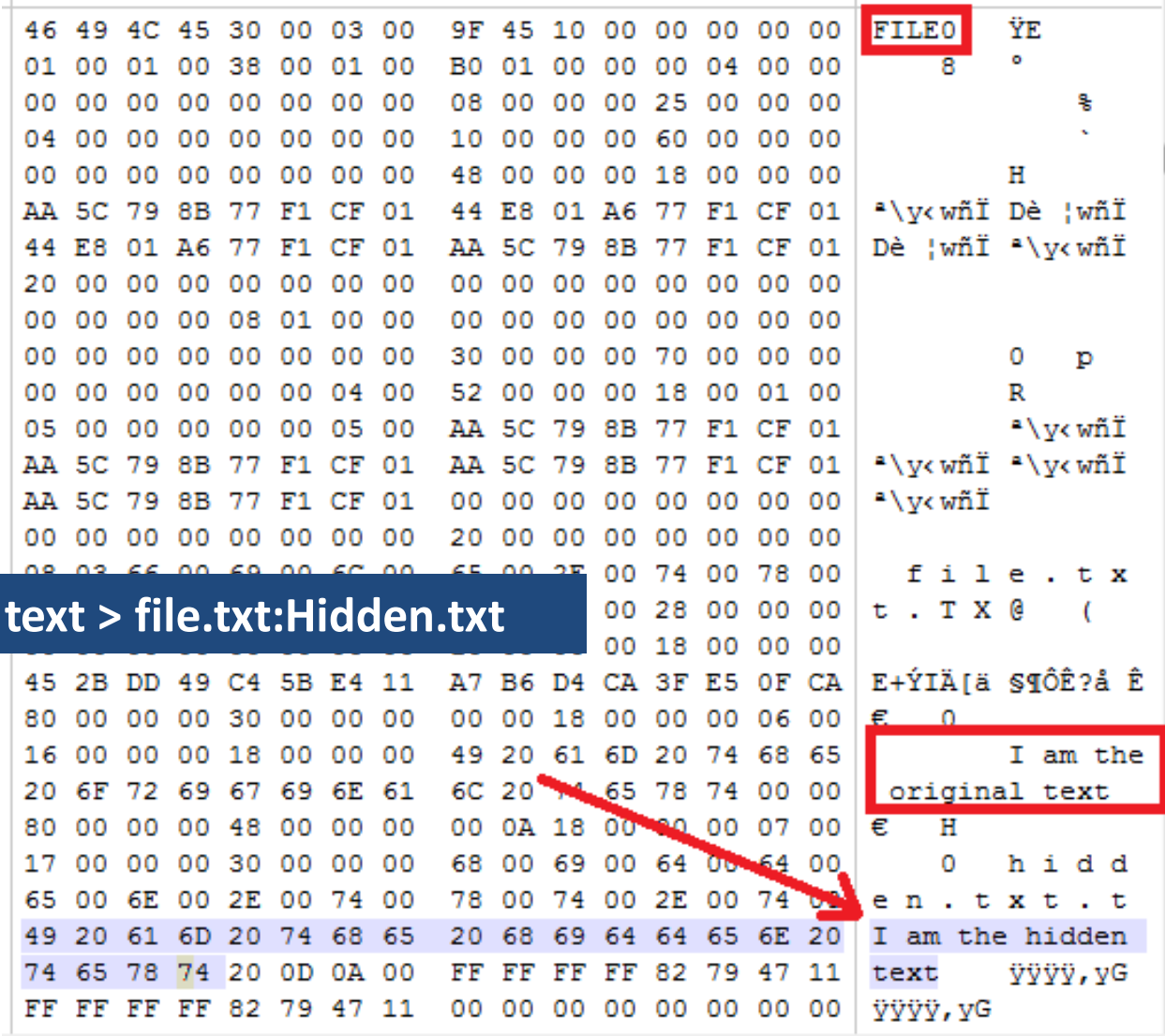
Bad Blocks ($BadClus)

- Marked in the metadata file **$BadClus** (*MFT entry 8*)
- Sparse file with the size set to the size of the entire file system
- Bad clusters are allocated to this file
- Clusters can be allocated to **$BadClus** and used to store data

Alternate Data Streams (ADS)

- More than one $DATA attribute
- Locating streams:
  - Streams, LADS, etc
  - DF tools
  - Manually

```
echo I am the hidden text > file.txt:Hidden.txt
```



ADS – Cont.

- Can also hide binaries!
  - Images
  - EXEs
  - etc

Isn't that evil or what?

Time Manipulation (Timestomp)

- Also a form of Data Hiding!

MFT#	MFTPrnt	CTime	ATime	MTime	RTime	FileName
10978	10456	2014-09-10 15:27:28:207:9439	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:207:9439	2014-09-10 15:27:28:207:9439	groucho.art
10979	10456	2014-09-10 15:27:28:248:0015	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:248:0015	2014-09-10 15:27:28:248:0015	holly.art
10980	10456	2014-09-10 15:27:28:298:0735	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:298:0735	2014-09-10 15:27:28:298:0735	ingrid.art
10981	10456	2014-09-10 15:27:28:348:1455	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:348:1455	2014-09-10 15:27:28:348:1455	jessie.art
10982	10456	2014-09-10 15:27:28:398:2175	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:398:2175	2014-09-10 15:27:28:398:2175	kathy.art
10983	10456	2014-09-10 15:27:28:448:2895	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:448:2895	2014-09-10 15:27:28:448:2895	kelly.art
10984	10456	2014-09-10 15:27:28:488:3471	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:488:3471	2014-09-10 15:27:28:488:3471	kennedy.art
10985	10456	2014-09-10 15:27:28:518:3903	1999-08-02 00:11:40:000:0000	2014-09-10 15:27:28:518:3903	2014-09-10 15:27:28:518:3903	kings.art
10986	10456	2014-09-10 15:27:28:568:4623	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:568:4623	2014-09-10 15:27:28:568:4623	kirk.art
10987	10456	2014-09-10 15:27:28:608:5199	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:608:5199	2014-09-10 15:27:28:608:5199	lincoln.art
10988	10456	2014-09-10 15:27:28:648:5775	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:648:5775	2014-09-10 15:27:28:648:5775	lovebox.art
10989	10456	2014-09-10 15:27:28:698:6495	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:698:6495	2014-09-10 15:27:28:698:6495	madonna.art
10990	10456	2014-09-10 15:27:28:748:7215	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:748:7215	2014-09-10 15:27:28:748:7215	monalisa.art
10991	10456	2014-09-10 15:27:28:788:7791	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:788:7791	2014-09-10 15:27:28:788:7791	newyears.art
10992	10456	2014-09-10 15:27:28:868:8943	1999-08-02 00:11:42:000:0000	2014-09-10 15:27:28:868:8943	2014-09-10 15:27:28:868:8943	oliver.art

Operating Systems

- Range from simple changing icons, names, file extensions, hide attrib, to known system names (svchost.exe), etc into more complex techniques leveraging the OS capabilities itself

- Changing the file extension
  - .doc → .xls
  - .pdf → .doc

- Hiding files within system directories

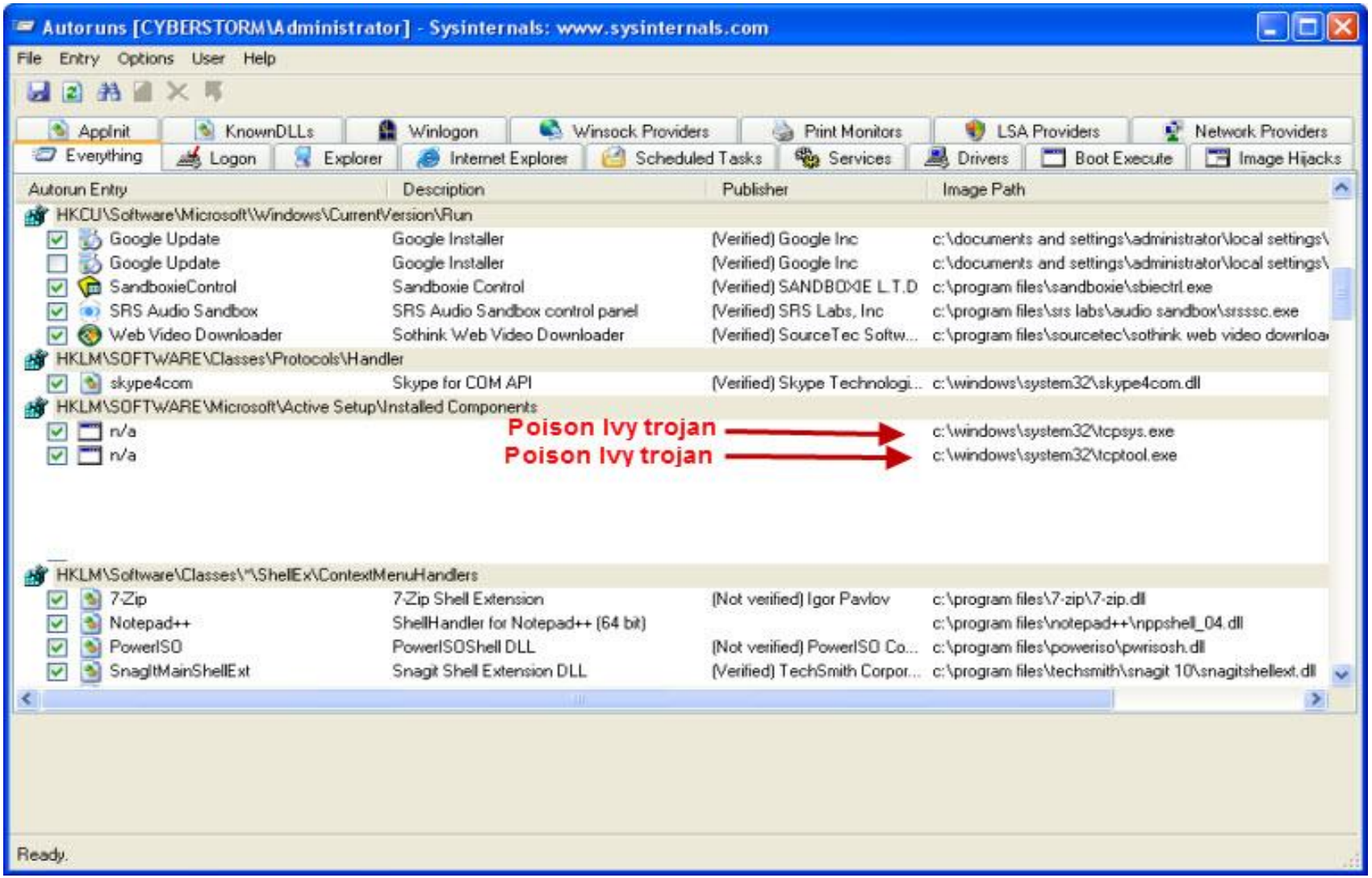
Operating Systems – Cont.

- System ACLs
- CLSIDs

rename FOLDER “My Computer.{20d04fe0-3aea-1069-a2d8-08002b30309d}”

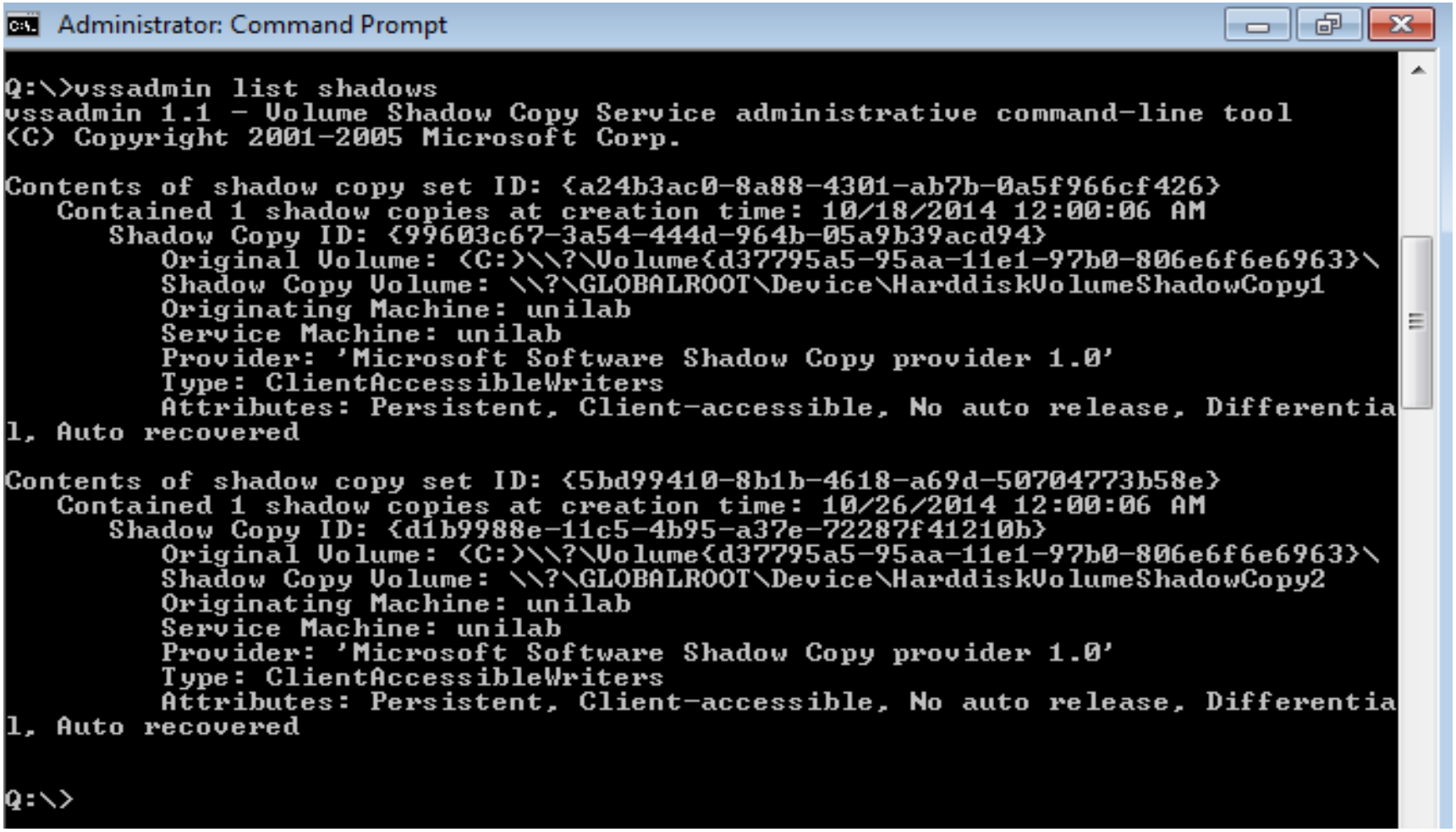
- Deleted Files and Removed Programs
  - Restore Points
  - Registry Entries
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Autoruns

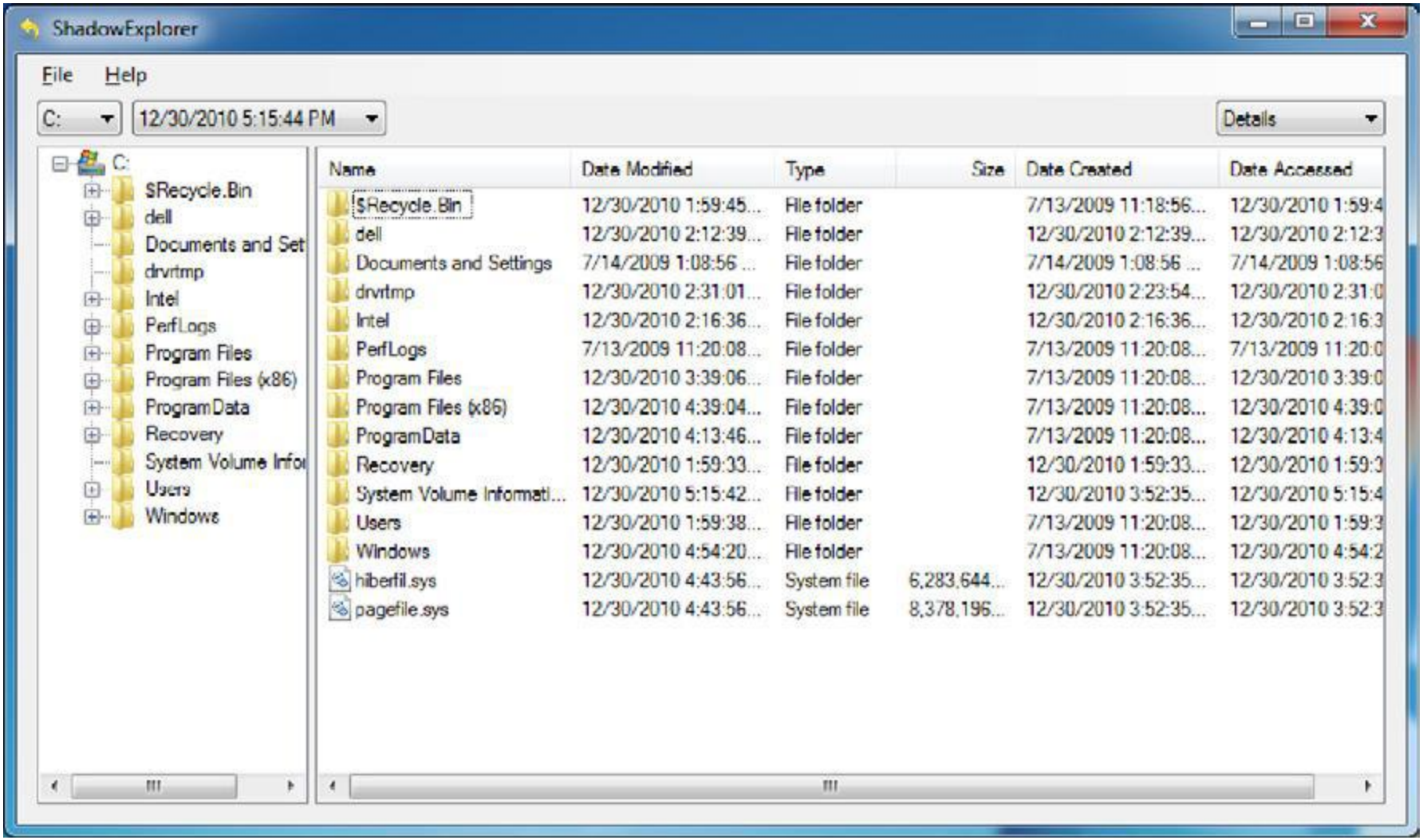

Autoruns [CYBERSTORM\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Boot Execute Image Hijacks
Autorun Entry Description Publisher Image Path
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Google Update Google Installer (Verified) Google Inc c:\documents and settings\administrator\local settings\
Google Update Google Installer (Verified) Google Inc c:\documents and settings\administrator\local settings\
SandboxieControl Sandboxie Control (Verified) SANDBOXIE L.T.D c:\program files\sandboxie\sbiectrl.exe
SRS Audio Sandbox SRS Audio Sandbox control panel (Verified) SRS Labs, Inc c:\program files\srs labs\audio sandbox\srsssc.exe
Web Video Downloader Sothink Web Video Downloader (Verified) SourceTec Softw... c:\program files\sourcetec\sothink web video downloa
HKLM\SOFTWARE\Classes\Protocols\Handler
skype4com Skype for COM API (Verified) Skype Technologi... c:\windows\system32\skype4com.dll
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
n/a
n/a
Poison Ivy trojan
Poison Ivy trojan
c:\windows\system32\tcpsys.exe
c:\windows\system32\tcptool.exe
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers
7-Zip 7-Zip Shell Extension (Not verified) Igor Pavlov c:\program files\7-zip\7-zip.dll
Notepad++ ShellHandler for Notepad++ (64 bit) c:\program files\notepad++\nppshell_04.dll
PowerISO PowerISOShell DLL (Not verified) PowerISO Co... c:\program files\poweriso\pwrisosh.dll
SnagItMainShellExt Snagit Shell Extension DLL (Verified) TechSmith Corpor... c:\program files\techsmith\snagit 10\snagitshellext.dll
Ready.

Operating Systems – VSC

- Volume Shadow Copies



Shadow Explorer – VSC Broswer



Covert Channels and Exfiltration

"Rules are made to be broken"

Intro.

- Any communication channel that can transfer information in a manner that violates a systems security policy

- **Goal:** hide the fact that a transmission is taking place

- **Why?**
  - Exfiltrate data from a secure system
  - Avoid detection of unauthorized access
  - Perform legitimate network management functions
  - Install, spread or control malware on compromised systems
  - Circumvent filters which may be in place limiting their freedom of speech
  - Bypass firewalls for unrestricted access to the web

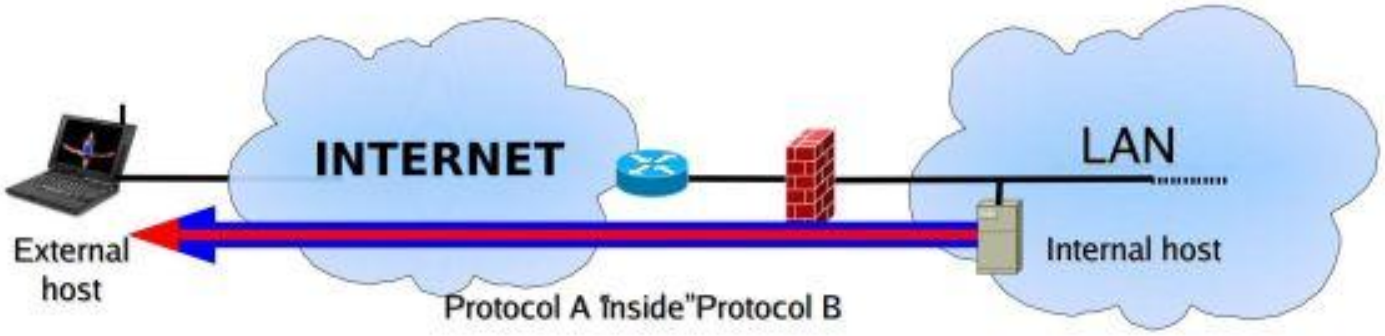
CC & Exfil

- Do you know what your network is sending/receiving?
- Any NSM, CIRT, SEIM, etc?

- **Exfiltrating Data Process:**
  - **Collect**: obtain required data
  - **Package**: obfuscate collected data to bypass IDS/IPS/DLP systems
  - **Exfil**: send packaged data using proper channels

Exfilitration: DNS

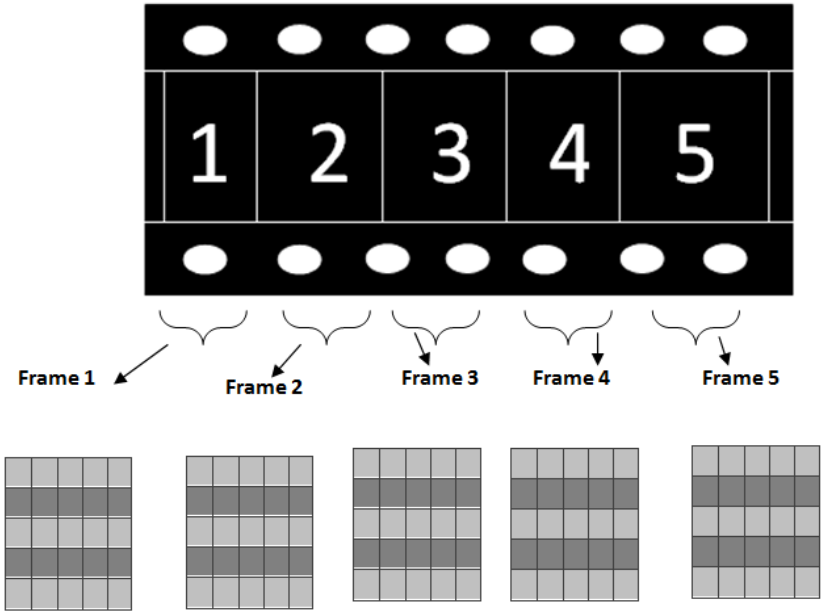
- One of the most un-monitored services is DNS!
- UDP 53 Indicators of Exfiltration
  - encrypted payloads or MD5, SHA1, SHA256 hashed subdomains
  - lots of requests to restricted domain or to one domain
  - DNS replies have private addresses or a single IP address
  - DNS replies have patterned encoding
  - etc

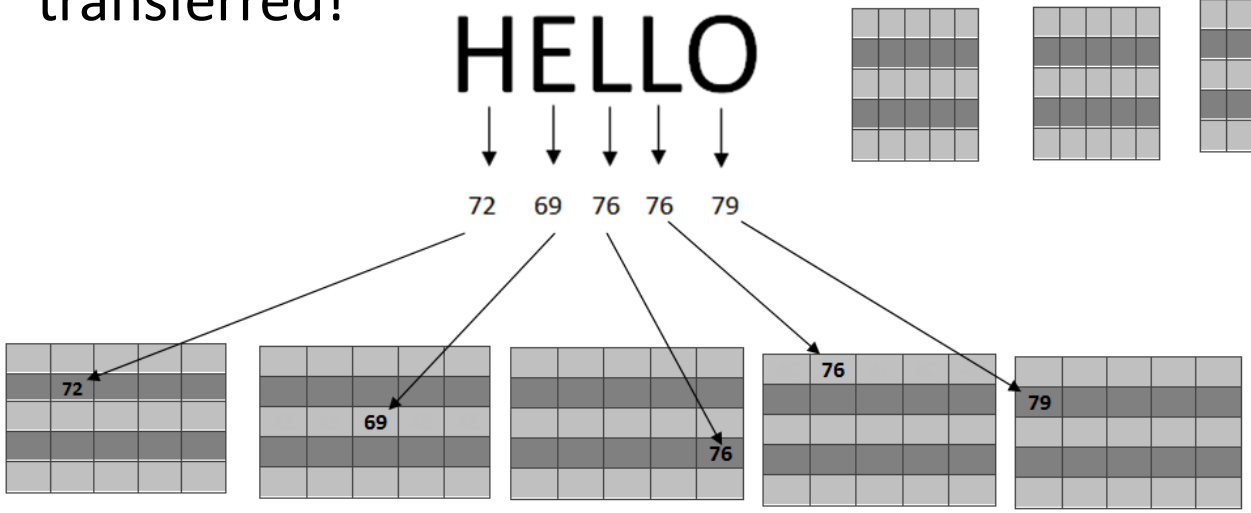


- Tools: dnscapy, dnstunnel, dftp, PSUDP, etc

Covert Channel: Under Your Radar

- Application layer covert channel
- Hide each letter in a single frame (steganography)
- No msg is actually transferred!

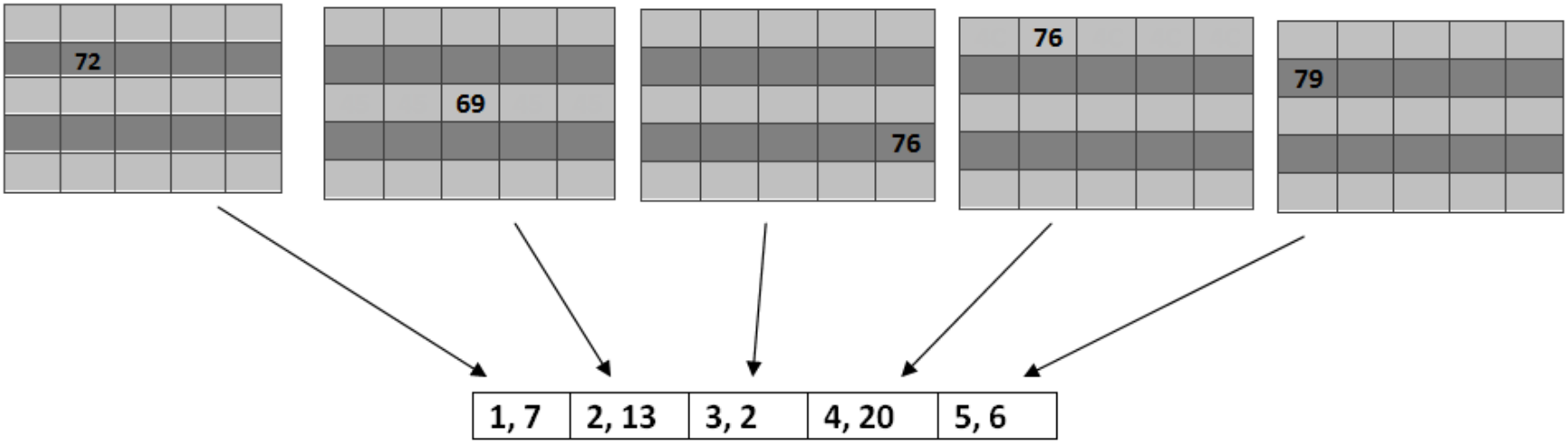


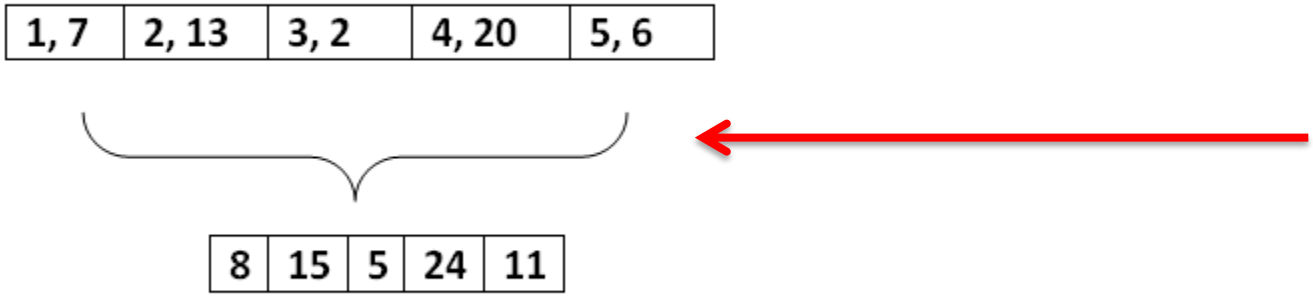


Research done by Mariam Khader under my supervision @PSUT

Under Your Radar (UYR)

- Save frame # and letter location

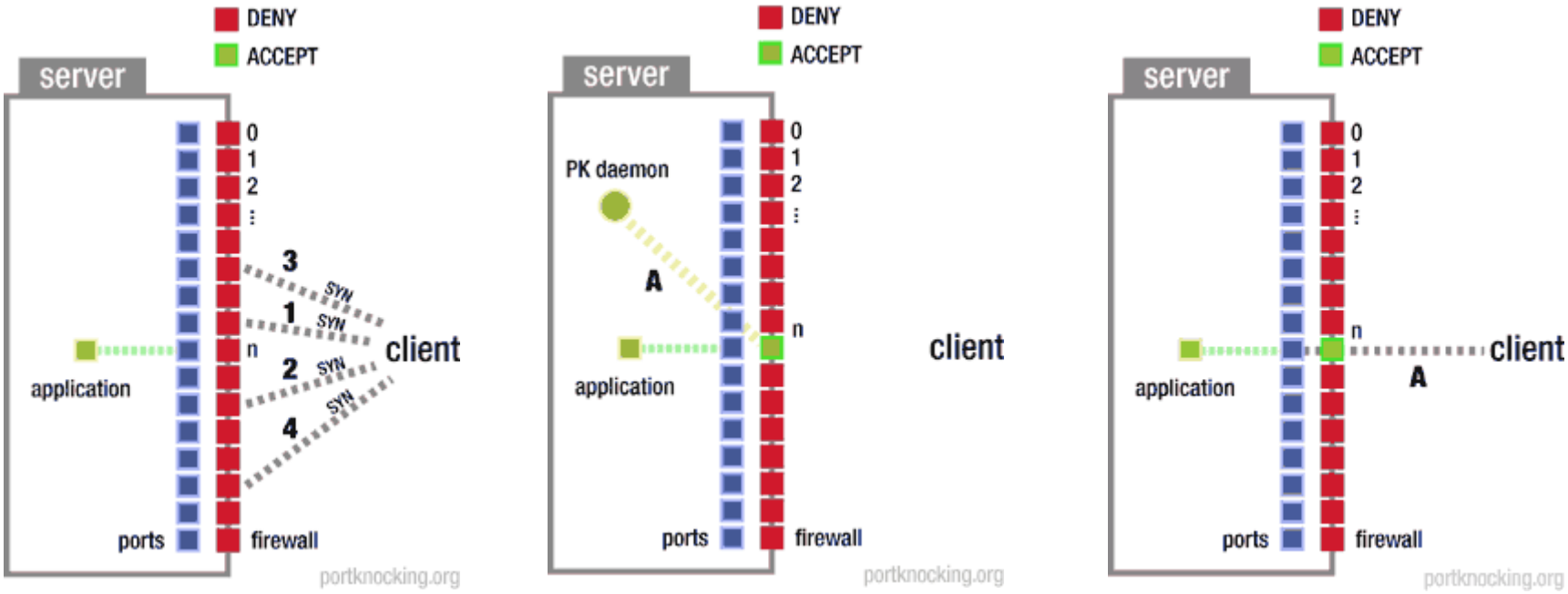




For further obfuscation

Covert Channel: TARIQ

- Hybrid Port Knocking System (my PhD research)
  - Used for host authentication
  - Makes network services completely invisible
  - Hidden feature: could be used as a covert channel



- How will you attack (exploit) an unseen service?

Anti-X and Binary Obfuscation

"What one man can invent, another can discover."

– Sherlock Holmes

Anti Forensics

- Locating anti-forensic tools leads to suspicion
  - Crumbs could be found even if removed!
  - Tools: StegoHunt, StegoAnalyst, StegoBreak, STG Cache Audit, Thumbnail Database Viewer, LNS, Streams (MS Sysinternals),

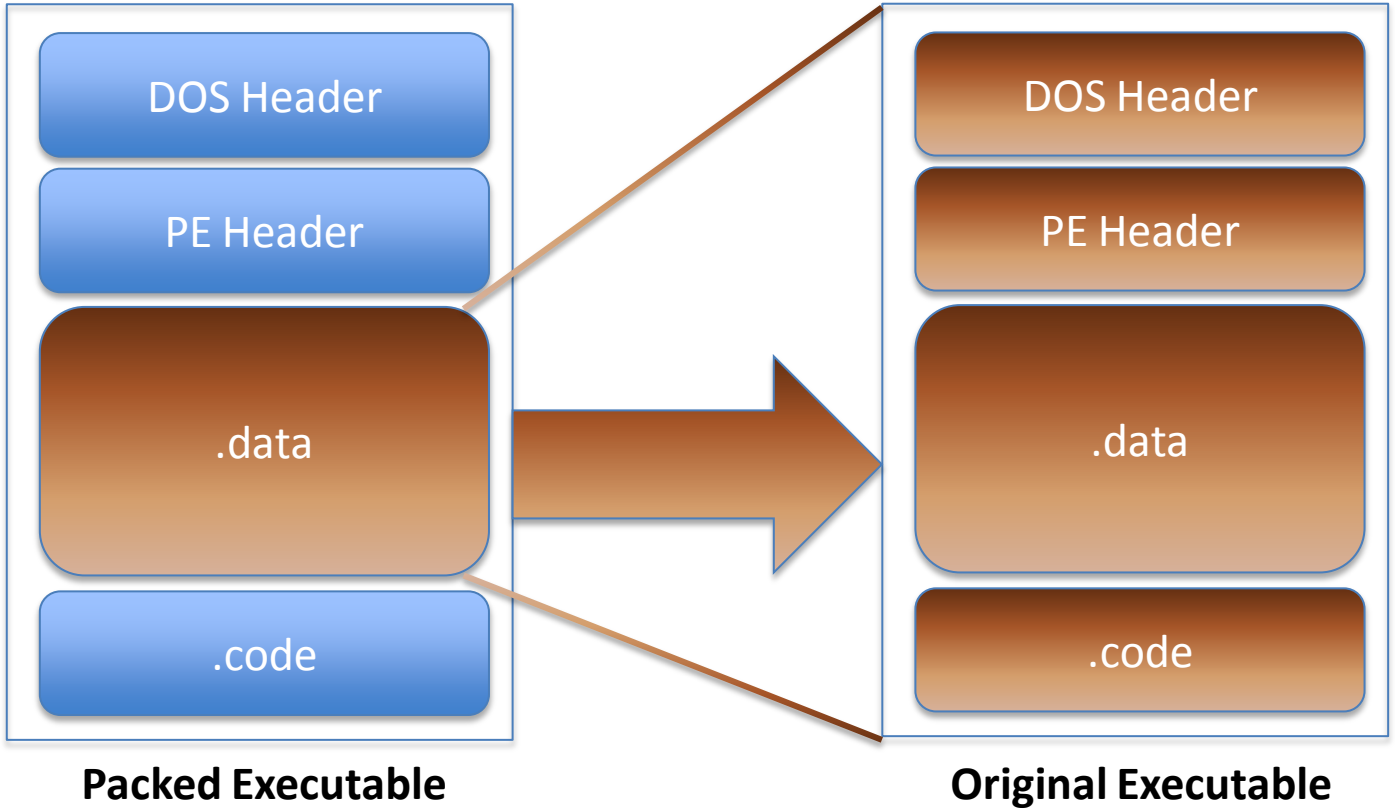
- **Simple:** clearing caches, offline files, app artifacts, deleting catalogs and thumbnail files, MRU and Jump Lists, Prefetch files, etc

- **Complex:** Full Disk Encryption, Anti-Debugging, Anti Reverse Engineering, Anti Disassembly, Anti-VM

Binary Obfuscation

- Packers / Unpackers
  - Reduce size, Hide actual code, Hide IAT, Anti-X

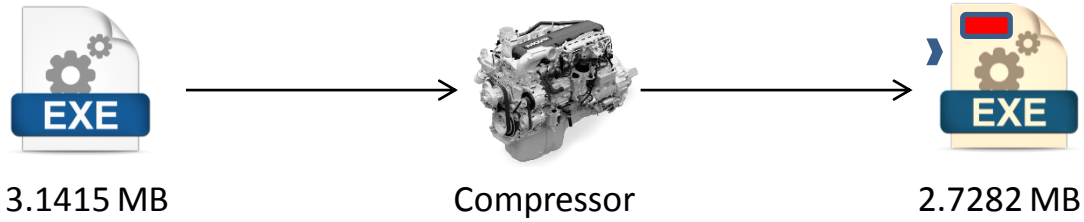
Simple Packer



Binary Obfuscation – Cont.

- Complex packers might overwrite its own memory space
- Unpacking:
  - Statically (complex and time consuming)
  - Dynamically (easy, needs native env.)
  - Hybrid (best of both)
- Types:
  - Common: UPX, FSG, MEW
  - Complex: Armadillo, Obsidium, Sdprotect, ExeCrypt, VMProtect

GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess



Finally …

- To catch a criminal, you must think like one
- Without proper understanding of the underlaying technology, its just like you're searching for a needle in the haystack!

References

- Syngress Data Hiding, 2013
- http://blogs.technet.com/b/askcore/archive/2013/03/24/alternate-data-streams-in-ntfs.aspx
- http://www.autohotkey.com/docs/misc/CLSID-List.htm
- http://marcoramilli.blogspot.com/2011/01/ida-pro-universal-unpacker.html
- http://www.woodmann.com/crackz/Packers.htm
- https://www.runtime.org/diskexplorer.htm
- http://www.portknocking.org/
- http://github.com/ashemery/tariq/
- One packer to rule them all, https://www.blackhat.com/docs/us-14/materials/us-14-Mesbahi-One-Packer-To-Rule-Them-All.pdf
- 13 Signs that bad guys are using DNS Exfiltration to steal your data, http://theworldsoldestintern.wordpress.com/
- http://cleanbytes.net/what-is-a-malicious-software-malware-and-how-to-detect-it/