Detecting Computer Intrusions: Are You Pwned?

Steve Anson
HITB
8 Oct 2009

Steve Anson

- **Former computer agent for the U.S. Department of Defense and Federal Bureau of Investigation (FBI) Cybercrime Task Force**
- **Former computer crime investigation instructor at the FBI Academy**
- **Co-author of *Mastering Windows Network Forensics and Investigations***
- **Instructor for U.S. State Department**
- **CISSP, MCSE, EnCE, blah, blah, blah**

Detecting Intrusions

Behavioral Indicators

Forensic Indicators

Initial Indicators

IDS / IPS Alert

- Sorting False Alarms Takes Time

Antivirus Alert

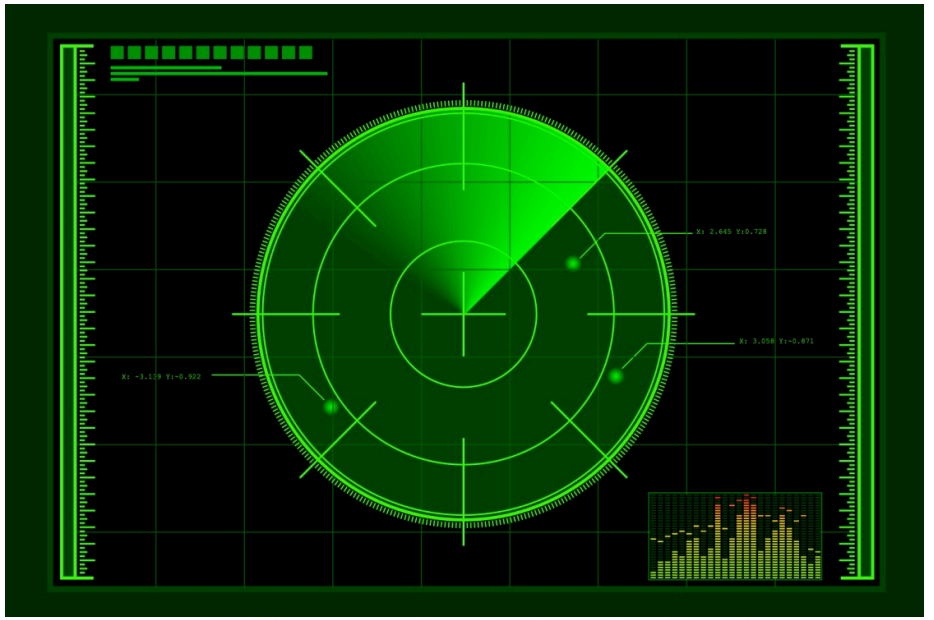
- Inbound or Already Installed?

SEIM Alert

- Again, Tricky to Configure

Behavioral Indicators

- **Scanning**
  - **Can be quite loud (lamers, worms)**
  - **Often more controlled (more dangerous)**



Behavioral Indicators

- **E.T. Phones Home**
  - **Beaconing**

Behavioral Indicators

- **The massive sucking sound of all your data leaving**
  - **Data exfiltration can be rapid and massive in scope**
  - **Attacker may stage for years and then pull data over one weekend**

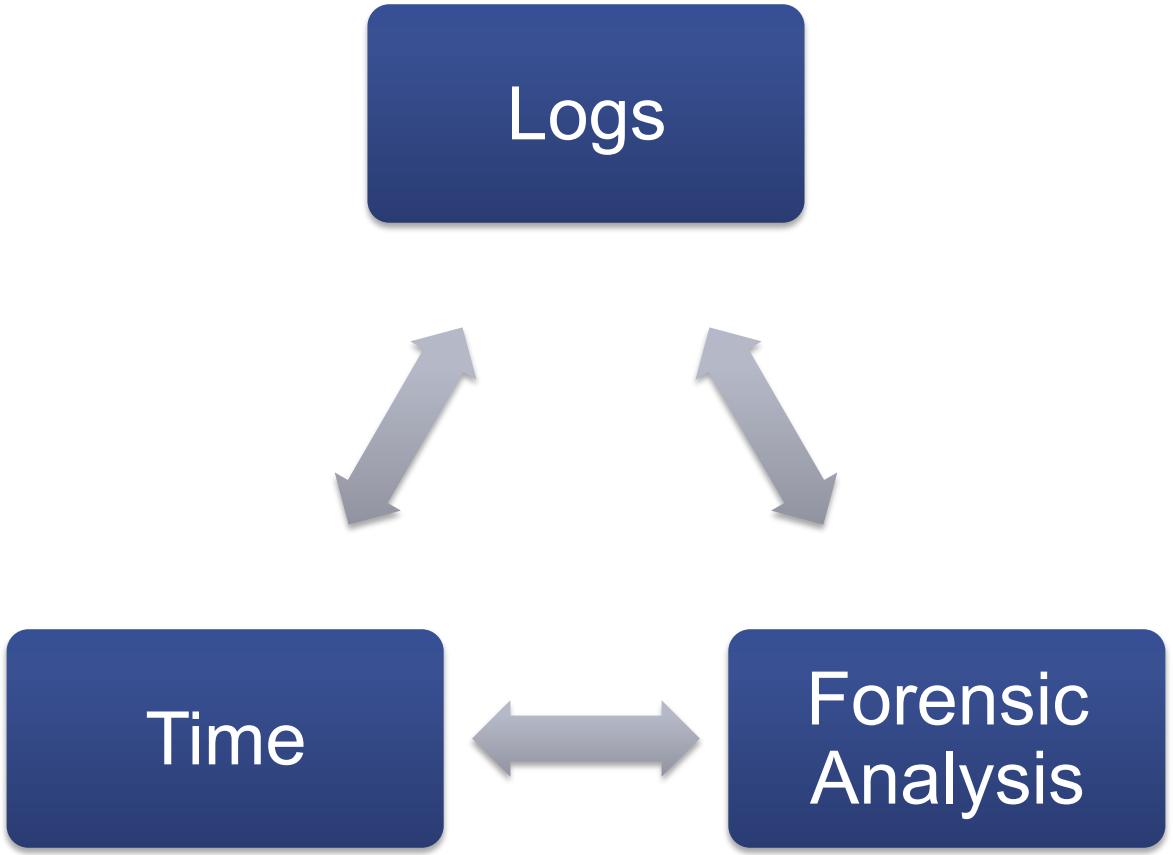
Behavioral Indicators

- **Traffic that's just not right**
  - **Large file transfers over port 53**
  - **Lots of extraneous SSL traffic**
  - **SSL traffic on port 80**

Behavioral Indicators

- **Unexplained user accounts**
  - **Old accounts that are reactivated**
  - **New accounts**
  - **Old accounts with new permissions**

Forensic Indicators



Logs

IDS / IPS

- Great if you've got them

Firewall

- Track connections in and out

Authentication Servers

- Unusual logon times or locations

Windows Logs

Remote Logon

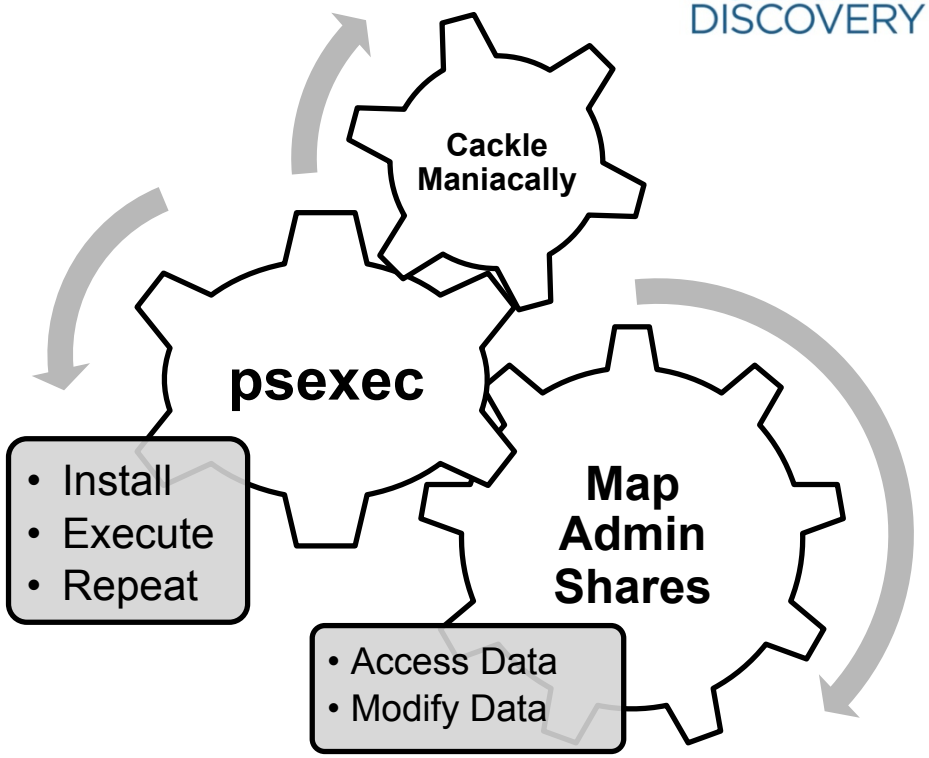
- **Event ID 528 (Logon Type 10), 540, 672, 673**

Event ID 7035, 7036

Password Guessing

- **Event ID 672 (Failure), 675, 676, 680, 681**

- So your network has the same or similar passwords for all local Administrator accounts?



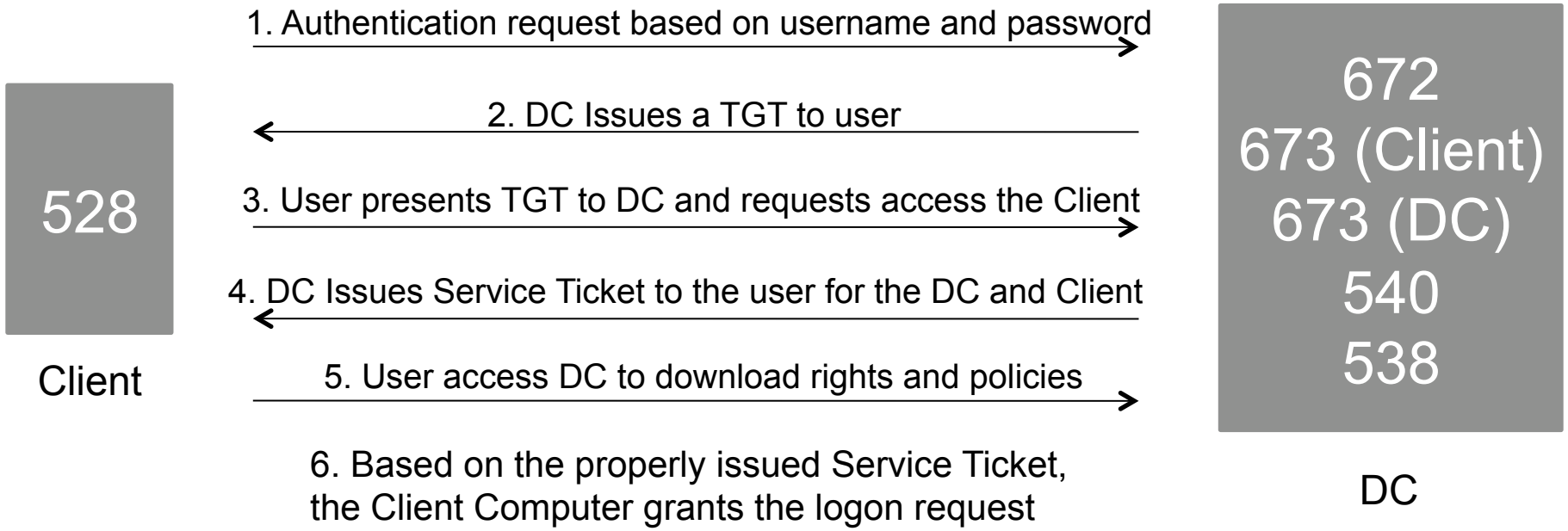
Windows Logs

- Windows records two categories of Events related to authentication and access

Logon Events	• Track access to resources (500s)
Account Logon Events	• Track authentication (600s)

Windows Logs

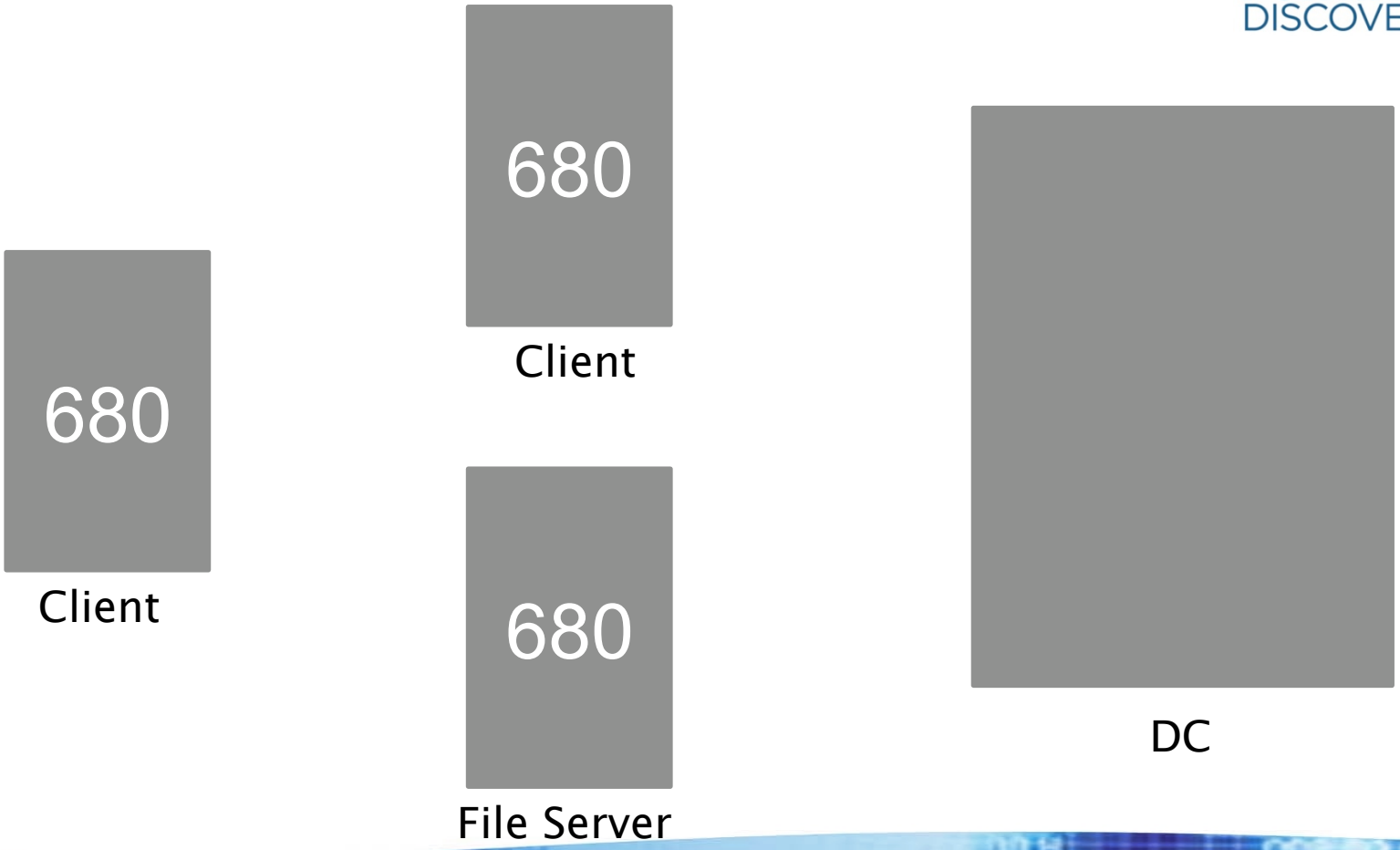
- Logging of Kerberos activity in a domain



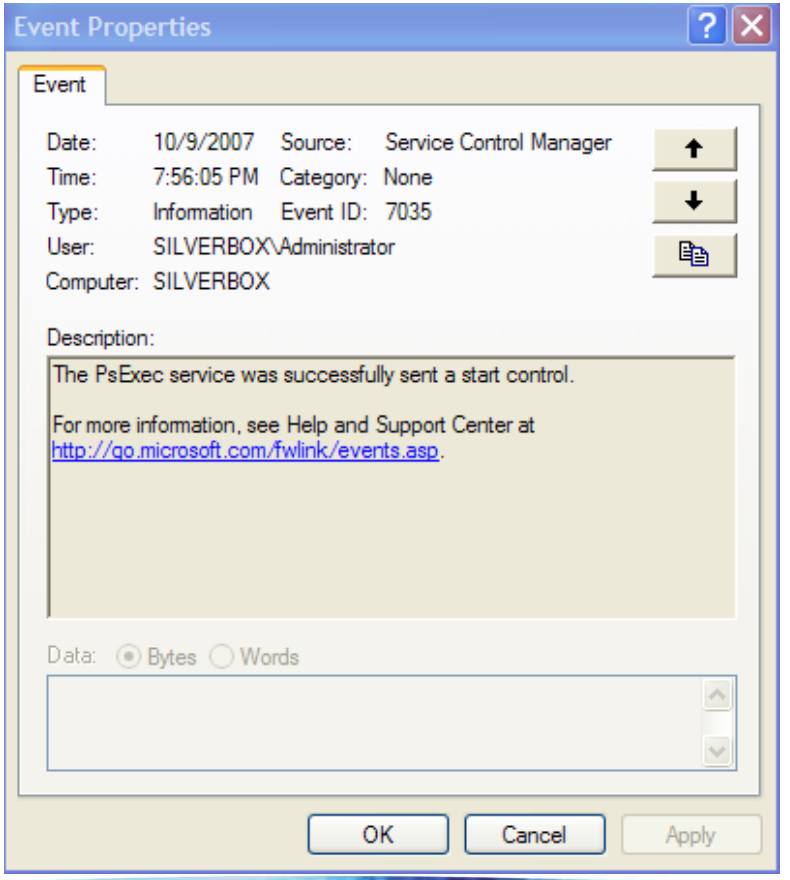
Windows Logs

- The use of local accounts in most domain environments is unusual
- Account Logon (authentication) events normally only appear on the DCs
- If local accounts are being used, Account Logon events will appear on individual computers

Windows Logs



- The use of psexec is very common once an attacker knows an account's password
- 7035 and 7036 events will be logged in System Log during psexec use



Is This Host 0wned?

- **Monitor Network Traffic**
- **Analyze Running Processes**
- **Forensically Image and Analyze**

Monitor Traffic

- **Monitor the machine**
- **Use historical logging if available**
- **Otherwise, use Wireshark, NetWitness Investigator, or similar product to capture traffic.**

Forensic Analysis

Memory Forensics

- **Running processes**
- **Open ports**
- **Active connections**
- **Malware only in RAM**

Forensic Analysis

Memory Forensics

- **Query RAM**
  - **netstat –ano (or netstat –anp)**
  - **tasklist /SVC (or ps –ef)**
  - **WinAudit, Process Monitor**
- **Dump RAM**
  - **HBGary, Volatility**

Forensic Analysis

Indicators of Evil

- **Close names**
  - **svvchost**
  - **svchosts**
- **Alternate locations**
- **Unexplained ports**

Example

WinAudit report showing two instances of Windows explorer, with slightly different names and very different sizes

Running Programs

Name	PID	Memory	Description
[System Process]	0		
AcroTray.exe	692	1764KB	AcroTray
alg.exe	2656	3300KB	Application Layer Gateway Service
csrss.exe	868	3540KB	
cvpnd.exe	1876	5180KB	Cisco Systems VPN Client
DefWatch.exe	120	1244KB	Virus Definition Daemon
dxplay.exe	1768	7636KB	Microsoft DirectX Diagnostic Tool
Explorer.exe	260	7008KB	Windows Explorer
explorer.exe	336	23784KB	Windows Explorer
hkcmd.exe	660	3636KB	hkcmd Module
lsass.exe	948	1664KB	LSA Shell (Export Version)
mysqld-nt.exe	1820	3100KB	

Example

“Explorer.exe” is listening on TCP port 19. Further, the path to “Explorer.exe” is abnormal, as it is normally in the root of Windows.

TCP 0.0.0.0:19

Item	Value
Port Protocol	TCP
Local Address	0.0.0.0
Local Port	19
Service Name	chargen
Remote Address	0.0.0.0
Remote Port	0
Connection State	Listening (LISTEN)
Process Name	C:\WINDOWS\addins\Explorer.exe
Process ID	260
Process Description	Windows Explorer
Process Manufacturer	Microsoft Corporation

Example

This same process (PID 260) is also listening on port 77

TCP 0.0.0.0:77

Item	Value
Port Protocol	TCP
Local Address	0.0.0.0
Local Port	77
Service Name	
Remote Address	0.0.0.0
Remote Port	0
Connection State	Listening (LISTEN)
Process Name	C:\WINDOWS\addins\Explorer.exe
Process ID	260
Process Description	Windows Explorer
Process Manufacturer	Microsoft Corporation

Example

And it's also listening on port 43958

TCP 127.0.0.1:43958

Item	Value
Port Protocol	TCP
Local Address	127.0.0.1
Local Port	43958
Service Name	
Remote Address	0.0.0.0
Remote Port	0
Connection State	Listening (LISTEN)
Process Name	C:\WINDOWS\addins\Explorer.exe
Process ID	260
Process Description	Windows Explorer
Process Manufacturer	Microsoft Corporation

Forensic Analysis

- **You've sniffed some traffic**
- **You've pulled some data from RAM**
- **Maybe you've performed external port scans**
- **Now image and analyze offline**

Forensic Imaging

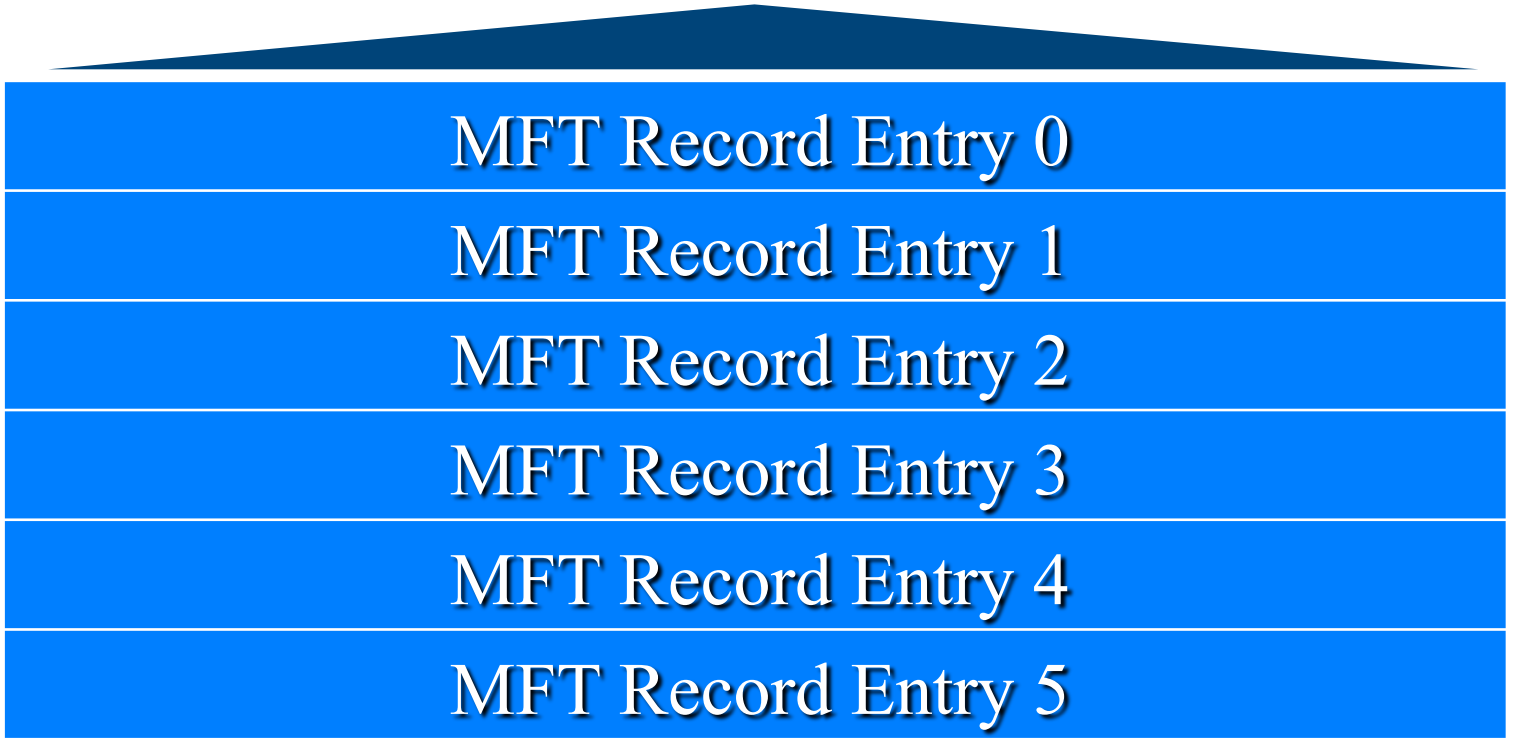
- **Helix**
- **Linen**
- **dcfldd**
- **Raptor**

Forensic Analysis

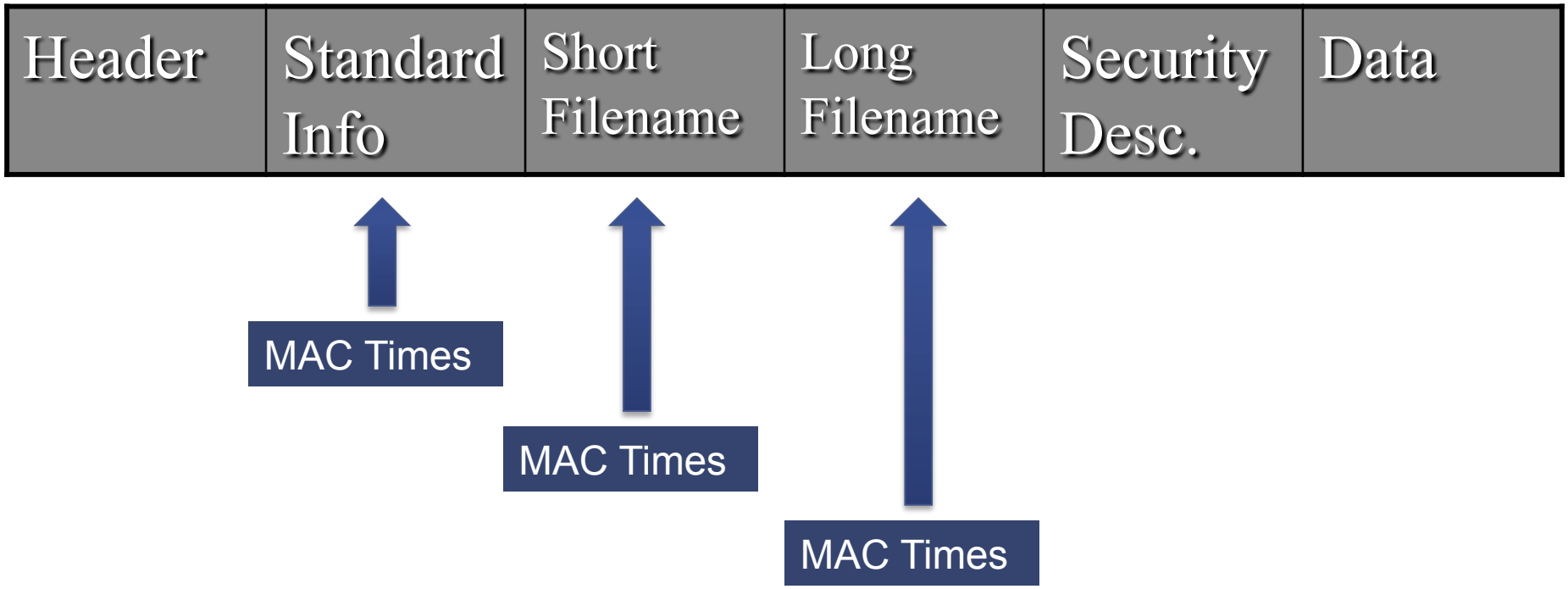
Timestamps

- **Standard of analysis**
- **Used to detect changes**
- **Some say its time has passed**

Forensic Analysis



Forensic Analysis



Forensic Analysis

Hash Analysis

- **MD5 or SHA1 hash comparisons**
- **Same limitation as any signature based solution**
- **Good at identifying other copies**
- **Good for eliminating known files**

Forensic Analysis

Binary Analysis

- **Extract File from Image**
- **Put in Sandbox or VM**
- **Execute and Monitor**
- **Disassembly**

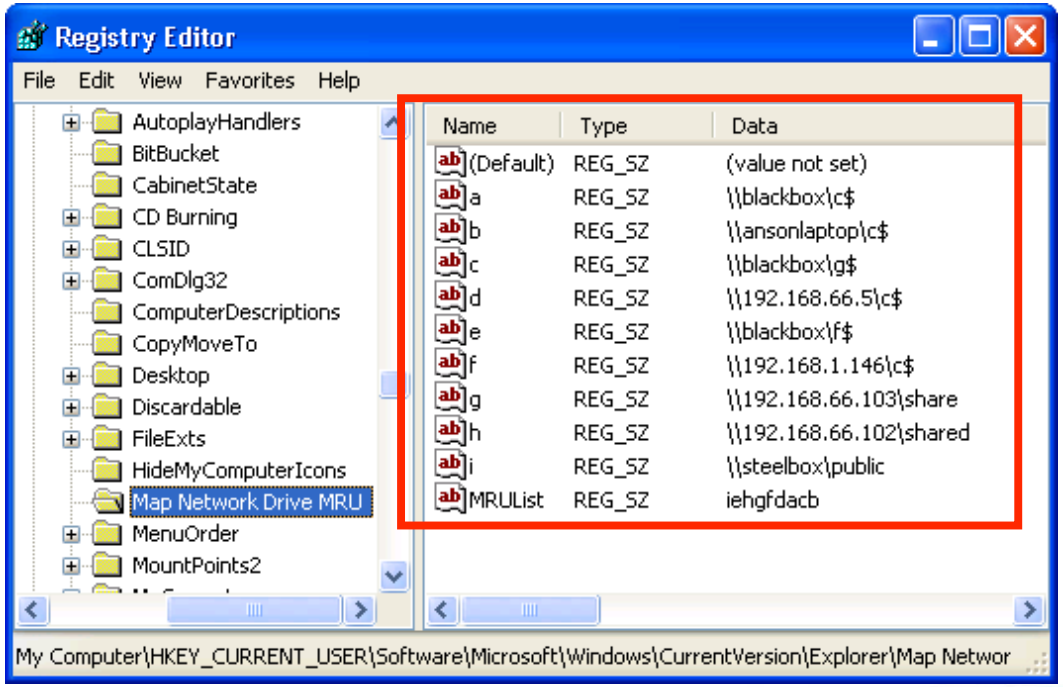
Forensic Analysis

Windows Registry

- **Stores useful information about system activity**
- **Can help detect compromised data and compromised systems**

NTUser.dat Data

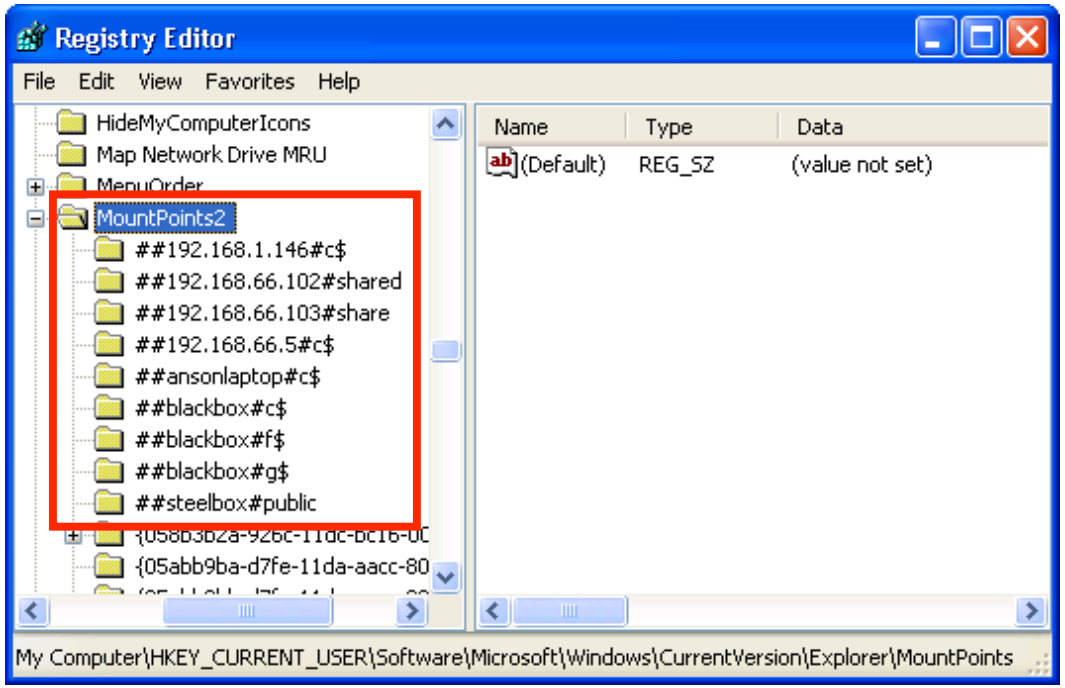
- Mapped Drives
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU



- Each mapped drive appears as a value with a letter as its name
- This is NOT the drive letter given to the drive when it was mapped
- The MRUList shows the order of mapping

NTUser.dat Data

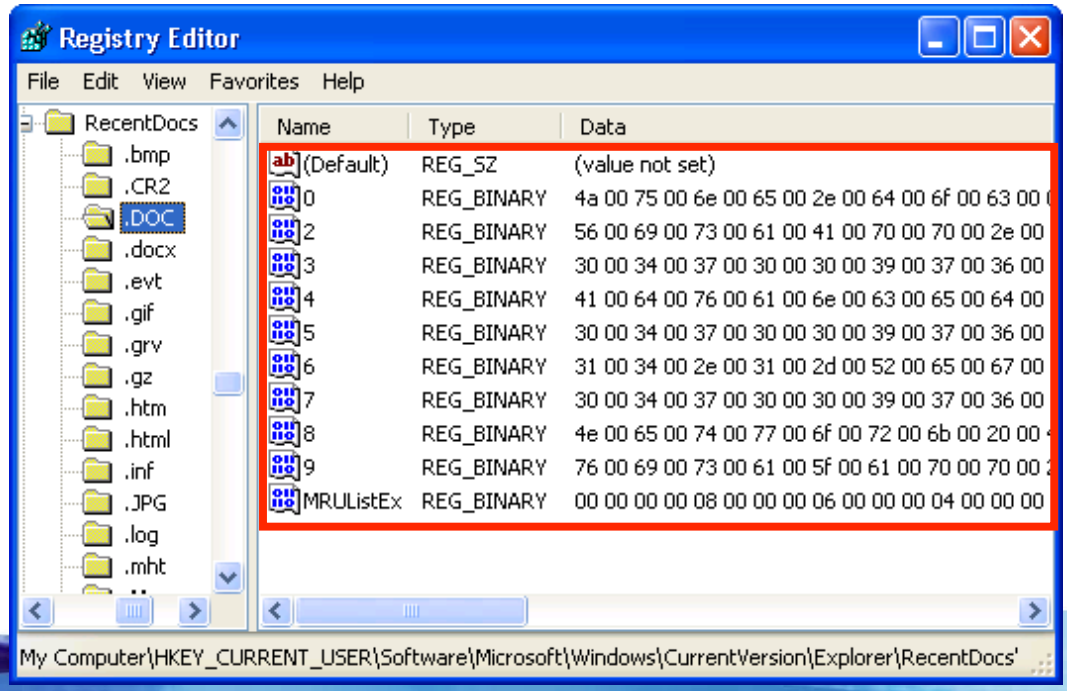
- HKCU\Software\Microsoft\Windows\ CurrentVersion \Explorer\MountPoints2



- Each subkey of the MountPoints2 key represents another device that was mounted to the system
- Share access to remote systems are recorded as ##hostname#share

NTUser.dat Data

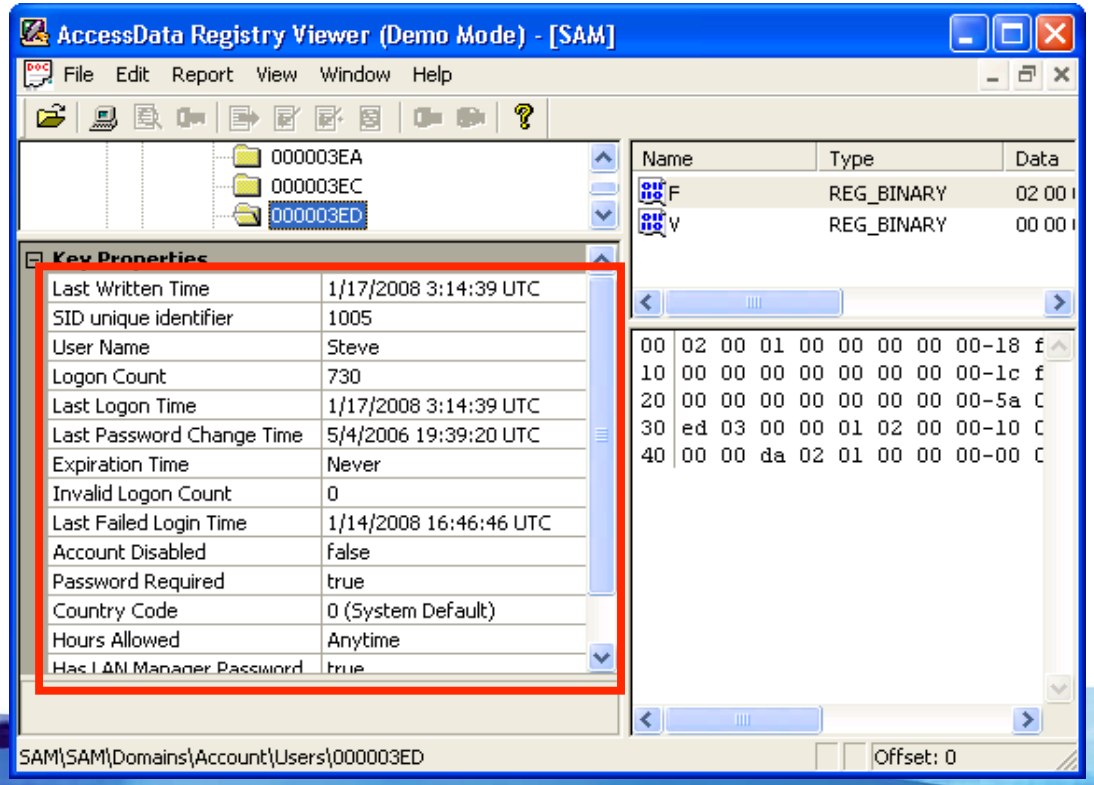
- Recently Accessed Documents
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



- Each file extension type gets its own subkey
- The values are given a number for a name
- The MRUListEx value shows the order of access

SAM Hive Data

- Typed URLs
- HKCU\SAM\Domains\Account\Users\<RID in hex>



- If multiple accounts have a “Last Failed Login Time” that is very similar, it may be indicative of password guessing attacks
- You can use this data to show when an account last logged in to the system

Enterprise Forensics

Contact Information

Steve Anson

Forward Discovery Middle East FZ-LLC

Dubai Knowledge Village

Block 6, Office F08

Mobile – +971 50 287 1062

Email – sanson@forwarddiscovery.com

Web – www.forwarddiscovery.com