CY5210 INFORMATION SYSTEM FORENSICS

Northeastern University

Module 8
Windows Event Logs

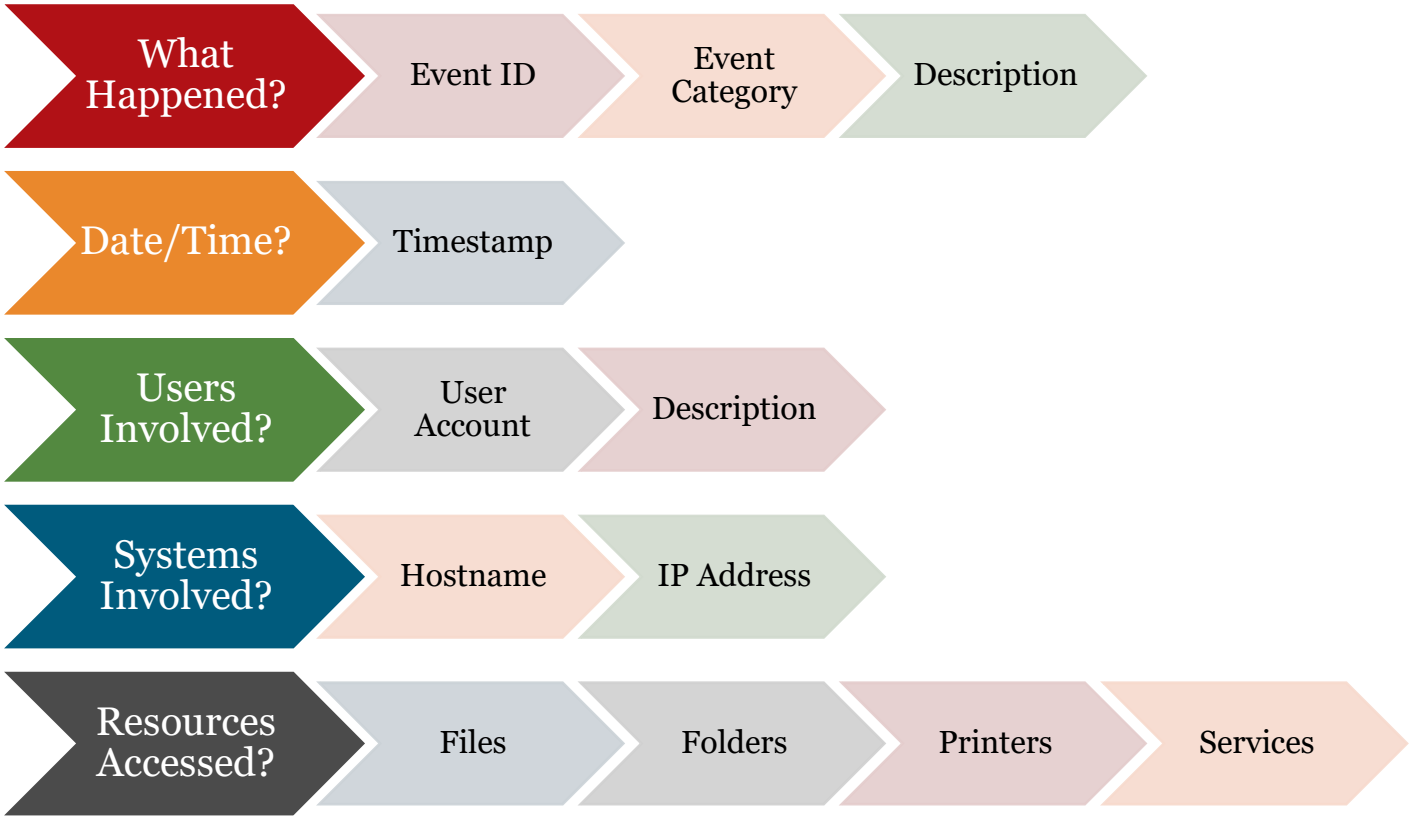
Elton Booker | Part-Time Lecturer | e.booker@northeastern.edu

Windows Events

- Centralized recording of information about:
  - Software
  - Hardware
  - Operating system functions
  - Security
- Multiple events comprise an *event log*

"Any significant occurrence in the system or in a program that requires users to be notified…"

Event Log Analysis



Windows Event Log Fundamentals

CY5210
Information System Forensics

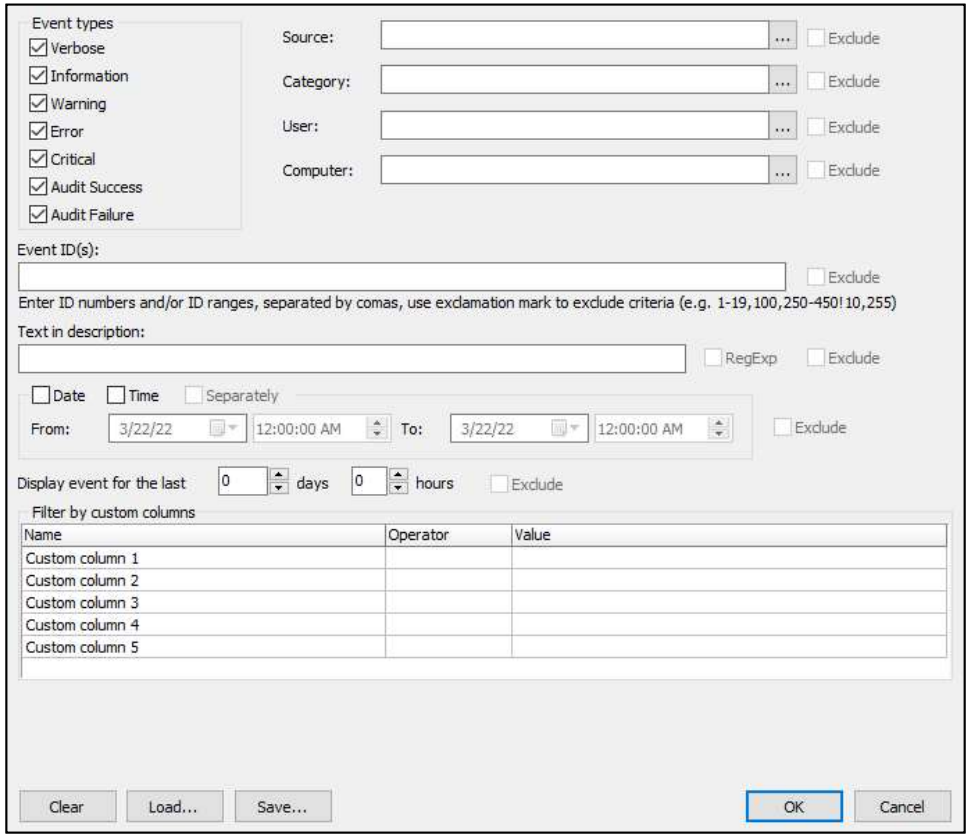
Event Log Locations

- **NT / Win2000 / XP / Server 2003**
  - .evt file type
  - %systemroot%\System32\config
  - Filenames: SecEvent.evt, AppEvent.evt, SysEvent.evt
- **Vista / Win7 / Win8 / 2008 / 2012 / Win10 / 2016 / 2019**
  - .evtx file type
  - %systemroot%\System32\winevt\logs
  - Potentially on remote log server
  - Filenames: Security.evtx, Application.evtx, System.evtx, etc

Default locations can be changed in the registry

.evtx Log Format

- Memory efficiencies
  - Less costly to log
- XML and filtering
- Improved messaging
  - IP addresses
  - Event IDs changed
- Expanded number of event logs
  - Increased granularity of audit controls



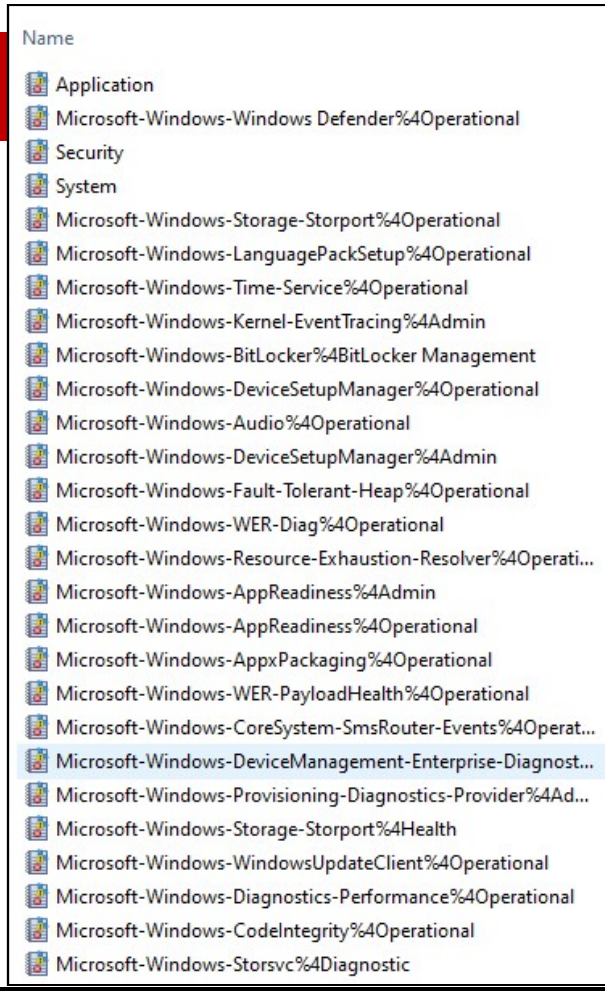
Types of Event Logs

Security	•Records access control and security settings information •Events based on audit and group policies •Example: Failed logon; folder access
System	•Contains events related to Windows services, system components, drivers, resources, etc. •Example: Service stopped; system rebooted
Application	•Software events unrelated to operating system •Example: SQL server fails to access a database
Custom	•Custom application logs •Examples: Server logs, including Directory Service, DNS Server, File Replication Service, Task Scheduler, PowerShell, WMI, and Firewall

Applications and Services Logs

- Stored in same folder as standard event logs: **%systemroot%\System32\winevt\Logs**
- In addition to Application, System, and Security, we now have many more logs to potentially review
- Logs often go further back in time than System, Security, and Application logs

Setup	•Records installation and update information for Windows
Forwarded Events	•Repository for events retrieved from other systems
Applications and Services	•Contains over 60 logs •Useful logs include Task Scheduler, Remote Desktop, Windows Firewall, and Windows Defender



Security Log

- Most reviewed log in Windows for incident response/forensics
  - User authentication and logon
  - User behavior and actions
  - File/Folder/Share access
  - Modifications of security settings
- Failure and success can be audited
  - Detailed logging can be enabled on specific user accounts
- Only updated by the LSASS process
  - Third-party applications cannot insert events

Security Event Categories: What is Recorded?

Local System Time

Account Logon	Events stored on system that authorized a **logon** event (DC or local system)
Account Management	Account maintenance and modifications
Directory Service	Attempted access of Active Directory objects
Logon Events	Each instance of logon/logoff on **local** system
Object Access	Access to objects identified in system access control list
Policy Change	Change of user rights, audit policies, or trust policies
Privilege Use	Each case of an account exercising a user right
Process Tracking	Process start, exit, handles, object access, etc.
System Events	System restart and shutdown; actions affecting the Security log

Default Security Logging

	Workstation	Workstation Recommended	Server	Server Recommended
Account Logon		Success/Failure		Success/Failure
Account Mgmt	Success	Success/Failure	Success	Success/Failure
Directory Service				DC Only
Logon Events	Success	Success/Failure	Success	Success/Failure
Object Access				
Policy Change	Success	Success/Failure	Success	Success/Failure
Privilege Use				Success/Failure
Detailed Tracking		Success		Success
System Events	Success/Failure	Success/Failure	Success/Failure	Success/Failure

Event Types

Error	•Significant problem; loss of data or functionality •Example: Server fails to load
Warning	•Not significant, but could indicate a future problem •Example: Low disk space
Information	•Successful operation of application, driver, or service •Example: Event Log Service was started
Success Audit	•Audited security event completed successfully •Example: Successful user logon
Failure Audit	•Audited security event did not complete successfully •Example: Failed access to a network drive

Windows Event Log Analysis Scenarios

CY5210
Information System Forensics

Analysis Scenario Examples

- Profiling Account Usage
- Analyzing File and Folder Access
- Time Manipulation
- Tracking BYOD and External Devices
- Geolocation Information

Tracking Account Usage (1)

- **Incident Response/Forensic Use Case**
  - Determine which accounts have been used for attempted logons
  - Track account usage for known compromised accounts

- **Relevant Event IDs**
  - **4624**: Successful Logon
  - **4625**: Failed Logon
  - **4634/4647**: Successful Logoff
  - **4672**: Account logon with superuser rights (Administrator)

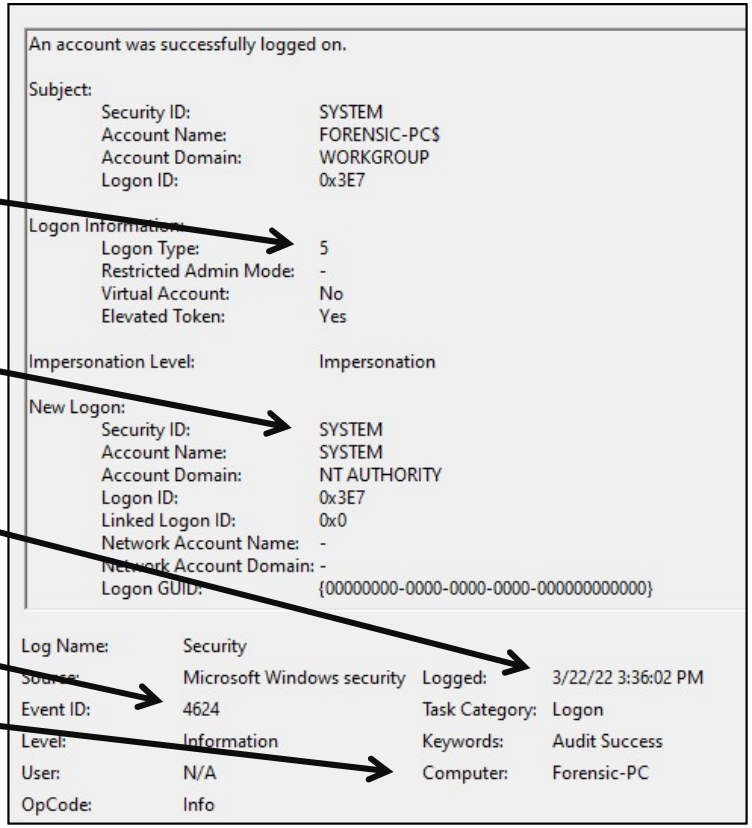
- **Investigation Relevance**
  - Event descriptions provide granular view of logon information
  - Windows does not record logoffs (4634) reliably so check interactive (4647)
  - Logon events not recorded by backdoors, exploited services, etc.

Tracking Account Usage (Security Log)

- **Incident Response/Forensic Use Case**
  - Determine which accounts have been used for attempted logons
  - Track account usage for known compromised accounts
- **Relevant Event IDs**
  - **4624**: Successful Logon
  - **4625**: Failed Logon
  - **4634/4647**: Successful Logoff
  - **4648**: Logon using explicit credentials (RunAs)
  - **4672**: Account logon with superuser rights (Admin)
  - **4720 / 4726**: An account was created / deleted
- **Investigation Relevance**
  - Event descriptions provide granular information
  - Windows does not record logoffs (ID 4634) reliably (check ID 4647)
  - Logon events not recorded by backdoors, exploited services, etc.

Tracking Account Usage (2)

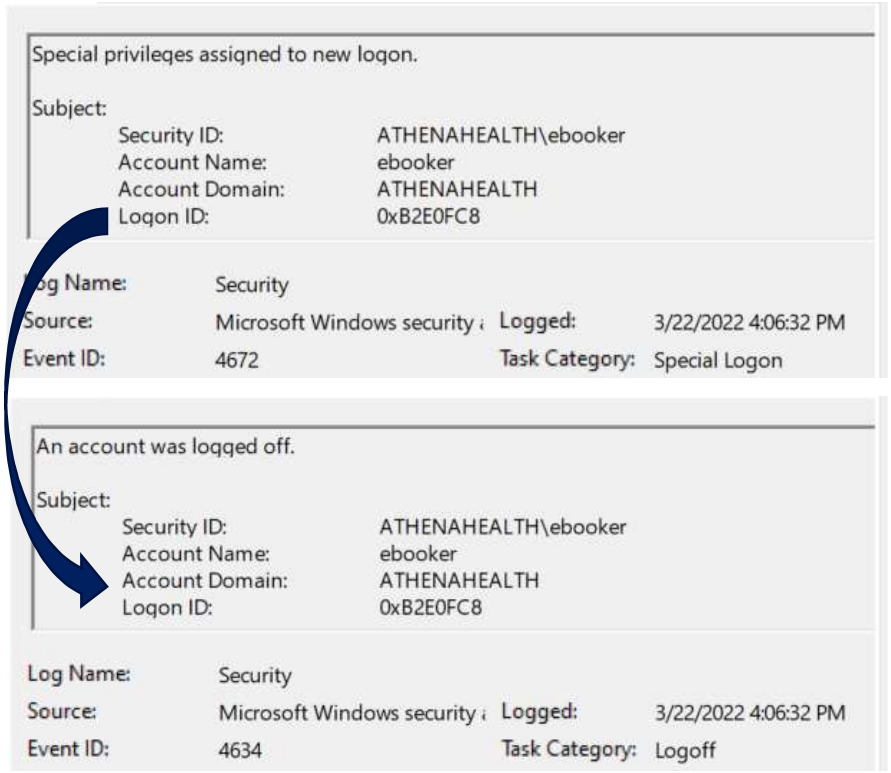
- **Logon Type**
- **Account**
- **Timestamp**
- **Event ID**
- **Computer**



Logon Type Codes

Logon Type Code	Explanation
2	Log on via console (keyboard, server KVM, or virtual client)
3	Network Logon (e.g. SMB for drive mapping)
4	Batch logon – used by Scheduled Tasks (non-interactive)
5	Windows Service Logon
7	Credentials used to lock or unlock screen; RDP session reconnect
8	Network logon sending credentials in cleartext
9	Different credentials used than logged on user – RunAs
10	Remote interactive logon (Remote Desktop Protocol)
11	Cached credentials used to log on (DC not available)
12	Cached Remote Interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

Identifying Logon Sessions



- Use the Logon ID value to link a logon with a logoff and determine session length
- Session time = **XX** mins

Tracking Account Usage Remote Desktop Protocol (1)

- **Incident Response/Forensic Use Case**
  - Track Remote Desktop Protocol logons to target machines

- **Relevant Event IDs**
  - **4778**: Session Reconnected
  - **4779**: Session Disconnected

- **Investigation Relevance**
  - Records hostname and IP address of source machine making the connection
  - Not a reliable indicator for **ALL** RDP activity due to "reconnects"
    - Valuable to fill in gaps snce RDP reconnects are often "Type 7" logons

  - Auxiliary logs ***Remote Desktop Services-RDPCoreTS*** and ***TerminalServices-RdpClient*** record complementary info

Analyzing File and Folder Access

- **Incident Response/Forensic Use Case**
  - Identify which users have attempted to access a protected file, folder, registry key, or other audited resource

- **Relevant Event IDs**
  - **4656**: Handle to object requested
  - **4660**: Object deleted
  - **4663**: Access attempt on object (read, write, delete, …)

- **Investigation Relevance**
  - Event includes timestamp, file/folder name, and account that attempted access
  - Filter by 4656 Failure Events to identify users attempting unauthorized access
  - Review 4663 events to identify what user actions occurred
  - Object auditing can quickly fill logs and requires tuning

Microsoft Office OAlerts (1)

- **Incident Response/Forensic Use Case**
  - Identify file interaction and alerts generated by Microsoft Excel, Word, Outlook, PowerPoint, Access, OneNote, and Publisher

- **Relevant Event IDs**
  - 300: Office Alert (used by all Office products)

- **Investigation Relevance**
  - Microsoft dialog alerts are recorded as events in OAlerts.evtx
  - File access, modification, and deletes may be recorded
  - Unauthorized access / permissions issues trigger events
  - Outlook activity is particularly valuable, as little other logging exists
  - OAlerts is not a comprehensive source of all Office activity

Time Manipulation (1)

- **Incident Response/Forensic Use Case**
  - Find evidence of time changes accomplished by user accounts
- **Relevant Event IDs**
  - **1**: Kernel-General (System log)
  - **4616**: System time was changed (Security log)
- **Investigation Relevance**
  - New Win8: **System** log events include user account information (previously only in Security log)
  - Security State Change Auditing must be enabled to log time changes into the **Security** log

Logs Related to Removable Devices

- **Incident Response/Forensic Use Case**
  - Determine what hardware devices have been installed on the system

- **Relevant Event IDs**
  - **20001**: Plug and Play driver install attempted (System log)
  - **4663**: Attempt to access removable storage object (Security log)
  - **4656**: Failure to access removable storage object (Security log)
  - **6416**: A new external device was recognized on system (Security log)

- Investigation Relevance
  - ***System*** log identifies device type and Serial Number but shows only ***first*** time a device was plugged in
  - ***Security*** log can identify ***every*** time a device is accessed and ***what*** files and folders were accessed (Win8+)

Wireless Network Geolocation (1)

- **Incident Response/Forensic Use Case**
  - Determine what wireless networks the system associated with and identify network characteristics to find location

- **Relevant Event IDs**
  - **11000**: Wireless network association started
  - **8001**: Successful connection to wireless network
  - **8002**: Failed connection to wireless network
  - **8003**: Disconnect from wireless network
  - **6100**: Network diagnostics (System log)

- **Investigation Relevance**
  - New custom log **Microsoft-Windows-WLAN-AutoConfig Operational.evtx**
  - Contains SSID and BSSID (MAC) that can be used to geolocate wireless AP

Event Log Summary

Artifacts	Location	Event IDs
Logons	Security	4624, 4625, 4634, 4647, 4672
RDP	Security | RDPCoreTS | TerminalServices-Remote	4778, 4779 | 131 | 1149
Object Access	Security | OAlerts	4656, 4660, 4663 | 300
Time Change	System | Security	1 | 4616
External Devices	System | Security	20001 | 4656, 4663, 6416
Wireless	WLAN-AutoConfig | System	8001, 8002, 11000 | 6100

Windows Event Log Resources

CY5210
Information System Forensics

Event Log Explorer

- Supports .evt and .evtx formats
- Can open multiple logs at once for simultaneous searching and correlation activities
  - Merge logs together to correlate
  - Access remote event logs

- Very tolerant of log corruption
- Excellent filtering
  - Strings in event description
  - Right-click for Quick Filters

- Color coding by Event IDs
- Free for personal use

Event Log Analysis Resources

- **Microsoft Security Log Documentation:**
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
- **Ultimate Windows Security**
  - https://www.ultimatewindowssecurity.com/
- **Eventopedia Windows Operating Systems**
  - http://eventopedia.cloudapp.net/Events/?/Operating+System/Microsoft+Windows
- **USB / Dropbox Reference Material**
  - Canvas or OneDrive