Path for Forensic Examiner Aces

Tuan Phan

CornCon Cybersecurity Conference

October - 2025

#Digital Forensics #DFIR

Introducing: Tuan Phan

Tuan works for a big well-known Financial institute...

As an Assistant Vice President (AVP) of eDiscovery and Forensics Examiner Lead and has many years of hands-on technical experience, including EF/DF/DFIR, and Insider Threat Strategy.

He is a Principal Security Engineer for

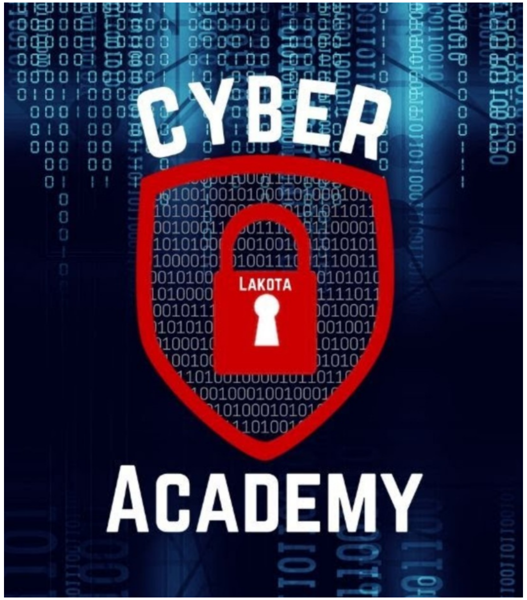
ThreatReel

https://threatreel.com

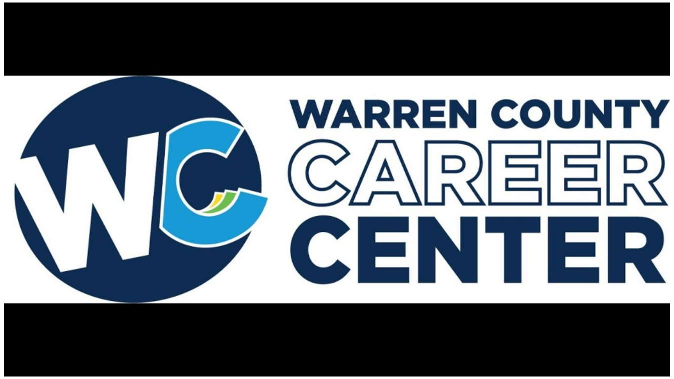
Follow / contact Tuan:

- https://www.linkedin.com/in/tuanqphan
- https://github.com/phanrensics/slides

Where I Volunteer...



Technical
Mentor



Advisory Board Member

Disclaimer!

Yes, the presenter have day jobs. However…

Opinions expressed are based solely on his own independent security research and do not express or reflect the views of his employers.

Agenda

What is a Digital Forensics Examiner (DFE)

- Baseline knowledge required for DFE
- Public vs Private
- Basic technical skills and the experience
- Q&A

“Forensic”

White Lab Coat

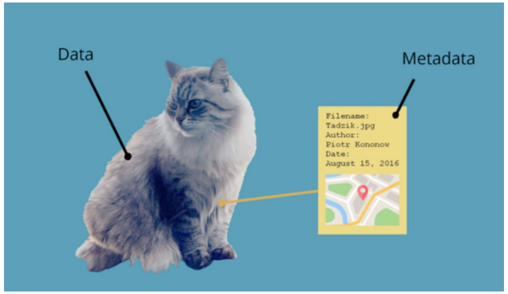
Clean Room\Forensic Lab

Why This Talk?

- This talk is inspired by job candidates I participated in interviewing.
- Help fill the knowledge, clear the confusion and skill gaps.
- Digital Forensics – Is this the career path for you?

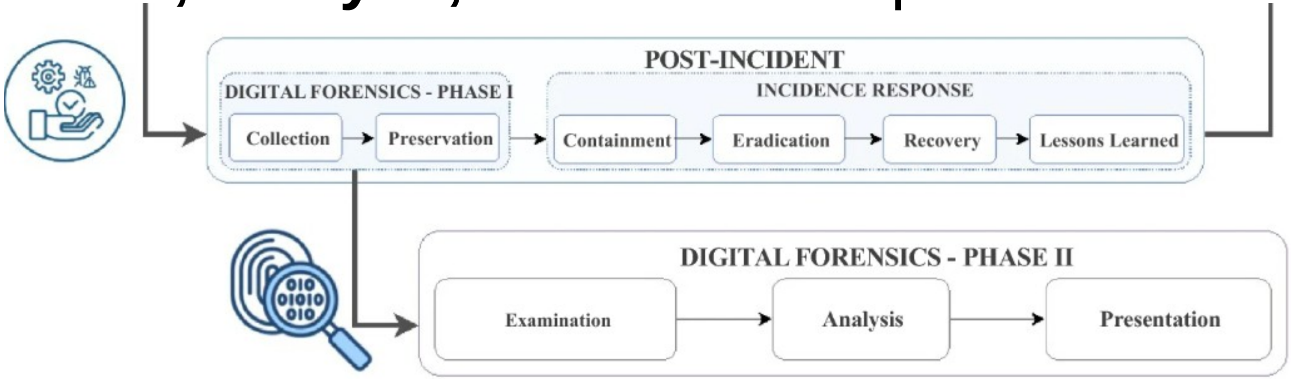
Digital Forensics

- **The process of identifying, collecting, preserving, extracting, analyzing, and presenting evidence.**
  - Manner that is legally acceptable, presented in a Court of Law or other.
- **Data is collected without alteration,**
  - Every step can be traced for legal and compliance purposes.
- **Reconstruction of events provide evidence of crimes or case of user misconduct.**
- **Data and Metadata**
  - **Author\Owner**
  - **Creation date**
  - **Modify date**
  - **Last Access date**
  - **Printed date**



Roles of DF\DFIR

- **Digital Forensics Examiner or Digital Forensics Incident Response (DFIR)**, both investigate security incidents, events, and alerts to answer the classic **“Who?”, “What?”, “When?”, “Where?”, “Why?”, and “How?”** questions.



POST-INCIDENT

DIGITAL FORENSICS - PHASE I

Collection → Preservation

INCIDENCE RESPONSE

Containment → Eradication → Recovery → Lessons Learned

DIGITAL FORENSICS - PHASE II

Examination → Analysis → Presentation

- **DF** essentially the collection, **preservation**, and analysis of data.

Aspiring DFE

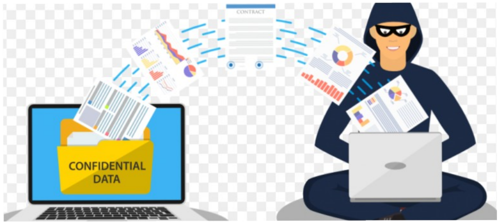
- Retain a working level knowledge of the 5 steps of digital forensics.

1) Identification
2) Data collection\preservation
3) Analysis & Examination
4) Reporting\Presentation
5) ***Documentation**

When Digital Forensic Starts

Tied to some kind of criminal or Cyber crime investigation.

- Any events that happen in your company's perimeter.
  - Inappropriate conduct\Fraud
  - Data being tampered\thief
  - Misuse of company resources
  - Someone getting access to something that they shouldn't have had or in a malicious way.
    - Mouse jiggler



What Does it Takes to be a DFE

1) Analytical Thinking: Ability to piece together clues and draw conclusion from complex data.

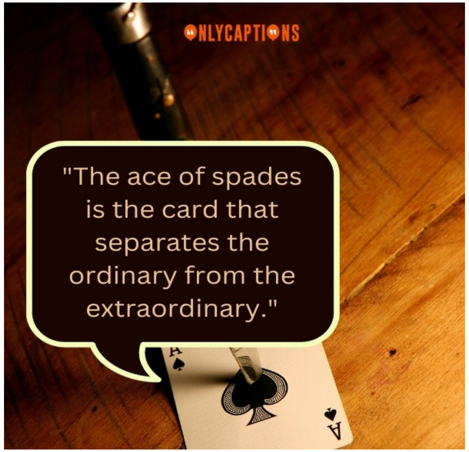
2) Attention to Detail: Precision is critical when handle and analyzing evidence.

3) Communication Skills: Teamwork and willingness to communicate and work well with others.

4) May work long hours.

5) Ability to be good under pressure.

6) *Testify in court.


ONLYCAPTIONS
"The ace of spades is the card that separates the ordinary from the extraordinary."

Public vs Private

Public Sector

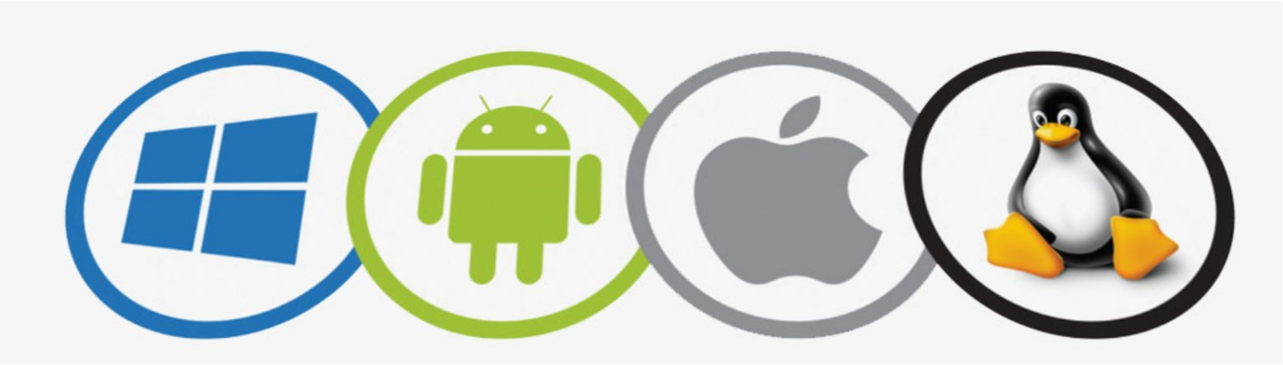
- Work with regional government bureaus
- Deal most with devices for evidence of criminal activities such as hacking, fraud, homicide, Drugs enforcement, Child abuse, and others.
- Goal is to provide evidence of crime.
- Lab Accreditation for ISO 9001

Private Organization

- Deal the same types of device analyses as public, but less intense in mobile volume.
- Email archives, SIEM, EDR, Compliance Portal, DLP, and other enterprise tools.
- Legal Right Hold (LRH)\eDiscovery -
  - FRCP Rule 37
- Goal is to solve the case of the user and prevent potential future threats.
- Not all lab are Accreditation for ISO 9001

OS Basic Skills

- **General knowledge of operating systems;**
  - Windows,
  - Linux & Mac
  - IOS
  - Android
  - Others



Basic Artifacts Skills

- **Windows:**
  - Recycle Bin/Deleted data, Registry, Browser artifacts, File Activity, winevt, SRUM, and others.
- **Linux & Mac:**
  - Trash Bin, File System Events, Browser artifacts, File Activity, *.plist, Recently Used Items, KnowledgeC: Application Focus, and others
- **Mobile devices (iOS\Android):**
  - Geo-location, communication, application, media, web browser, and others

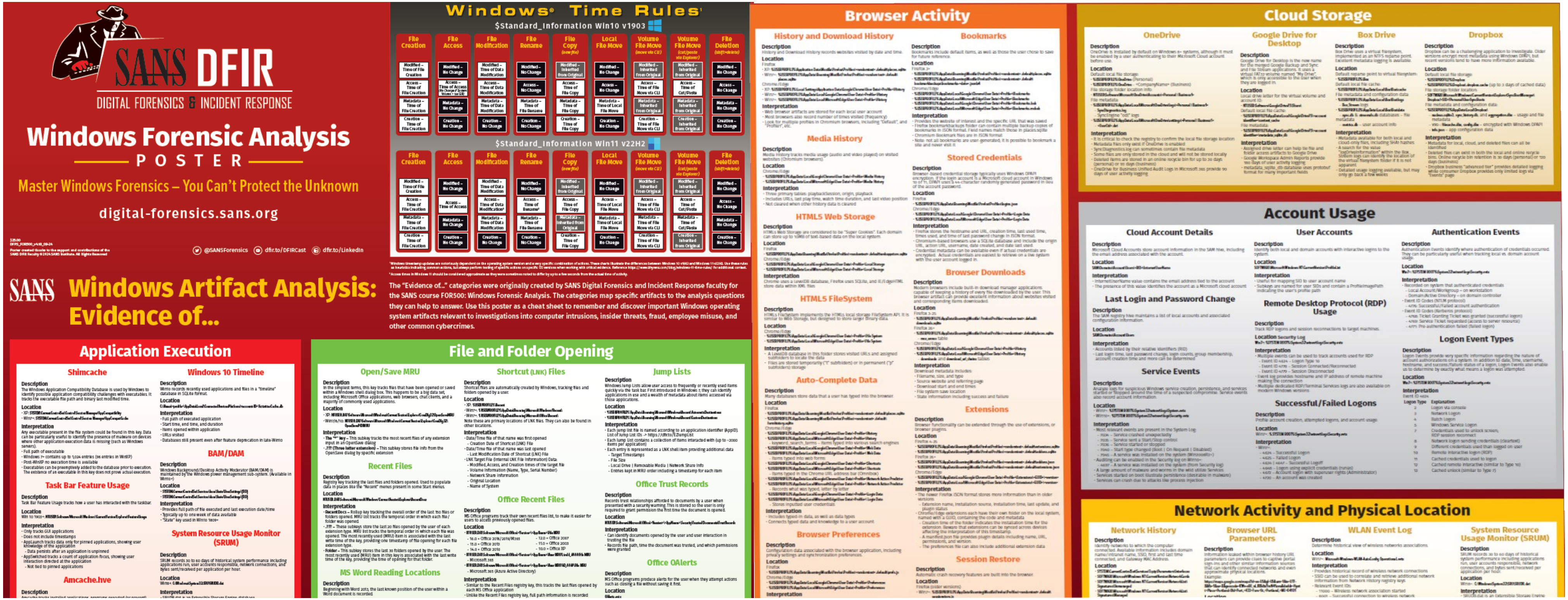
File-system Basic Skills

Knowing where things are supposed to be located on an endpoint\devices

Windows • C:\Recycle.bin • \Windows\System32\Config\*registry • \Windows\System32\sru\SRUDB.dat • \Users\AppData\Local\ConnectedDevicesPlatform\<id>\ActivitiesCache.db	**Linux\Mac** • /home/<USERNAME> • /etc, /var/log, and /etc/passw • *.plist
IOS • /mobile/Library/Safari/ • /mobile/Library/SMS/sms.db • /mobile/Library/CallHistoryDB/	**Android** • /system/packages.list • /system_ce/0/recent_images • /data/system/usagestats/0

Windows Forensic Analysis Poster

https://www.sans.org/posters/windows-forensic-analysis/



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis
POSTER

Master Windows Forensics – You Can't Protect the Unknown

digital-forensics.sans.org

@SANSForensics dfir.to/DFIRCast dfir.to/LinkedIn

Windows Time Rules

$Standard_Information Win10 v1903

$Standard_Information Win11 v22H2

File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move	Volume File Move (cut/paste via Explorer)	File Deletion

SANS Windows Artifact Analysis: Evidence of...

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incident Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map specific artifacts to the analysis questions they can help to answer. Use this poster as a cheat sheet to remember and discover important Windows operating system artifacts relevant to investigations into computer intrusions, insider threats, fraud, employee misuse, and other common cybercrimes.

Application Execution

Shimcache

Windows 10 Timeline

BAM/DAM

Task Bar Feature Usage

System Resource Usage Monitor (SRUM)

Amcache.hve

File and Folder Opening

Open/Save MRU

Shortcut (LNK) Files

Jump Lists

Recent Files

Office Recent Files

Office Trust Records

MS Word Reading Locations

Office OAlerts

Browser Activity

History and Download History

Bookmarks

Media History

Stored Credentials

HTML5 Web Storage

Browser Downloads

HTML5 FileSystem

Auto-Complete Data

Extensions

Browser Preferences

Session Restore

Cloud Storage

OneDrive

Google Drive for Desktop

Box Drive

Dropbox

Account Usage

Cloud Account Details

User Accounts

Authentication Events

Last Login and Password Change

Remote Desktop Protocol (RDP) Usage

Logon Event Types

Service Events

Successful/Failed Logons

Network Activity and Physical Location

Network History

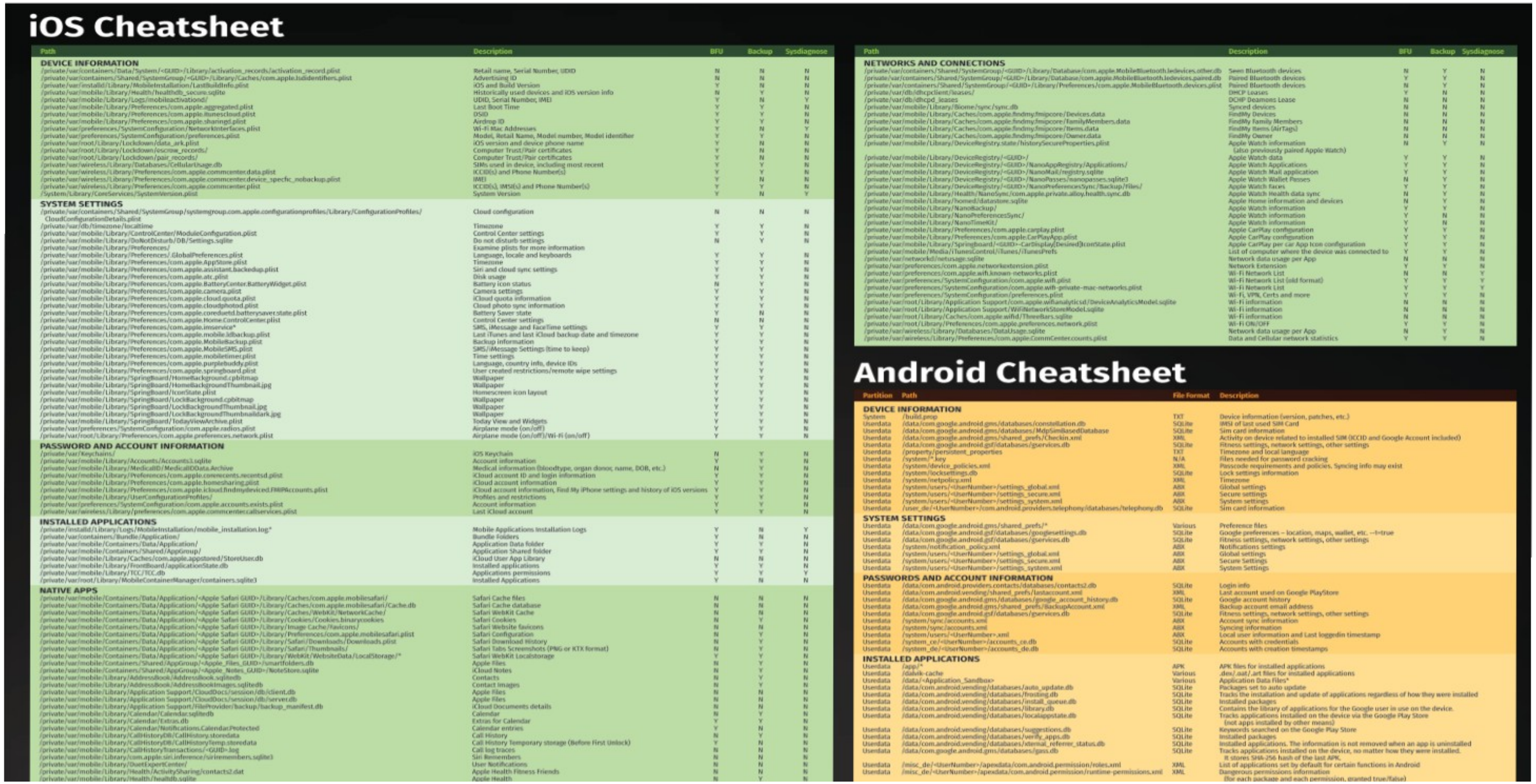
Browser URL Parameters

WLAN Event Log

System Resource Usage Monitor (SRUM)

Smartphone Forensics Posters

https://www.sans.org/posters/dfir-advanced-smartphone-forensics/



iOS Cheatsheet

Path	Description	BFU	Backup	Sysdiagnose
DEVICE INFORMATION				
/private/var/containers/Data/System/<GUID>/Library/activation_records/activation_record.plist	Retail name, Serial Number, UDID	N	N	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Caches/com.apple.lsdidentifiers.plist	Advertising ID	N	N	N
/private/var/installd/Library/MobileInstallation/LastBuildInfo.plist	iOS and Build Version	Y	N	N
/private/var/mobile/Library/Health/healthdb_secure.sqlite	Historically used devices and iOS version info	N	Y	N
/private/var/mobile/Library/Logs/mobileactivationd/	UDID, Serial Number, IMEI	Y	N	Y
/private/var/mobile/Library/Preferences/com.apple.aggregated.plist	Last Boot Time	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.itunescloud.plist	DSID	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.sharingd.plist	Airdrop ID	Y	Y	N
/private/var/preferences/SystemConfiguration/NetworkInterfaces.plist	Wi-Fi Mac Addresses	Y	N	Y
/private/var/preferences/SystemConfiguration/preferences.plist	Model, Retail Name, Model number, Model identifier	Y	Y	N
/private/var/root/Library/Lockdown/data_ark.plist	iOS version and device phone name	Y	N	N
/private/var/root/Library/Lockdown/escrow_records/	Computer Trust/Pair certificates	Y	N	N
/private/var/root/Library/Lockdown/pair_records/	Computer Trust/Pair certificates	Y	N	N
/private/var/wireless/Library/Databases/CellularUsage.db	SIMs used in device, including most recent	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.data.plist	ICCID(s) and Phone Number(s)	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.device_specfic_nobackup.plist	IMEI	Y	N	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.plist	ICCID(s), IMSI(s) and Phone Number(s)	Y	Y	N
/System/Library/CoreServices/SystemVersion.plist	System Version	Y	N	Y
SYSTEM SETTINGS				
/private/var/containers/Shared/SystemGroup/systemgroup.com.apple.configurationprofiles/Library/ConfigurationProfiles/CloudConfigurationDetails.plist	Cloud configuration	N	N	N
/private/var/db/timezone/localtime	Timezone	Y	Y	N
/private/var/mobile/Library/ControlCenter/ModuleConfiguration.plist	Control Center settings	Y	Y	N
/private/var/mobile/Library/DoNotDisturb/DB/Settings.sqlite	Do not disturb settings	N	Y	N
/private/var/mobile/Library/Preferences/	Examine plists for more information			
/private/var/mobile/Library/Preferences/.GlobalPreferences.plist	Language, locale and keyboards	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.AppStore.plist	Timezone	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.assistant.backedup.plist	Siri and cloud sync settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.atc.plist	Disk usage	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.BatteryCenter.BatteryWidget.plist	Battery icon status	N	Y	N
/private/var/mobile/Library/Preferences/com.apple.camera.plist	Camera settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.cloud.quota.plist	iCloud quota information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.cloudphotod.plist	Cloud photo sync information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.coreduetd.batterysaver.state.plist	Battery Saver state	Y	N	N
/private/var/mobile/Library/Preferences/com.apple.Home.ControlCenter.plist	Control Center settings	N	N	N
/private/var/mobile/Library/Preferences/com.apple.imservice*	SMS, iMessage and FaceTime settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobile.ldbackup.plist	Last iTunes and last iCloud backup date and timezone	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.MobileBackup.plist	Backup information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist	SMS/iMessage Settings (time to keep)	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobiletimer.plist	Time settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist	Language, country info, device IDs	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.springboard.plist	User created restrictions/remote wipe settings	Y	Y	N
/private/var/mobile/Library/SpringBoard/HomeBackground.cpbitmap	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/HomeBackgroundThumbnail.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/IconState.plist	Homescreen icon layout	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackground.cpbitmap	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackgroundThumbnail.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackgroundThumbnaildark.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/TodayViewArchive.plist	Today View and Widgets	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.radios.plist	Airplane mode (on/off)	Y	Y	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist	Airplane mode (on/off)/Wi-Fi (on/off)	Y	Y	N
PASSWORD AND ACCOUNT INFORMATION				
/private/var/Keychains/	iOS Keychain	N	Y	N
/private/var/mobile/Library/Accounts/Accounts3.sqlite	Account information	Y	Y	N
/private/var/mobile/Library/MedicalID/MedicalIDData.Archive	Medical information (bloodtype, organ donor, name, DOB, etc.)	N	Y	N
/private/var/mobile/Library/Preferences/com.apple.corerecents.recentsd.plist	iCloud account ID and login information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.homesharing.plist	iCloud account information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.icloud.findmydeviced.FMIPAccounts.plist	iCloud account information, Find My iPhone settings and history of iOS versions	Y	Y	N
/private/var/mobile/Library/UserConfigurationProfiles/	Profiles and restrictions	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.accounts.exists.plist	Account information	Y	Y	N
/private/var/wireless/Library/preferences/com.apple.commcentercallservices.plist	Last iCloud account	Y	Y	N
INSTALLED APPLICATIONS				
/private/installd/Library/Logs/MobileInstallation/mobile_installation.log*	Mobile Applications Installation Logs	Y	N	Y
/private/var/containers/Bundle/Application/	Bundle Folders	Y	N	N
/private/var/mobile/Containers/Data/Application/	Application Data folder	Y	Y	N
/private/var/mobile/Containers/Shared/AppGroup/	Application Shared folder	Y	Y	N
/private/var/mobile/Library/Caches/com.apple.appstored/StoreUser.db	iCloud User App Library	N	N	N
/private/var/mobile/Library/FrontBoard/applicationState.db	Installed applications	Y	Y	N
/private/var/mobile/Library/TCC/TCC.db	Applications permissions	Y	Y	Y
/private/var/root/Library/MobileContainerManager/containers.sqlite3	Installed Applications	Y	N	N
NATIVE APPS				
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Caches/com.apple.mobilesafari/	Safari Cache files	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Caches/com.apple.mobilesafari/Cache.db	Safari Cache database	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Caches/WebKit/NetworkCache/	Safari WebKit Cache	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Cookies/Cookies.binarycookies	Safari Cookies	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Image Cache/Favicons/	Safari Website favicons	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Preferences/com.apple.mobilesafari.plist	Safari Configuration	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Safari/Downloads/Downloads.plist	Safari Download History	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/Safari/Thumbnails/	Safari Tabs Screenshots (PNG or KTX format)	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID>/Library/WebKit/WebsiteData/LocalStorage/*	Safari WebKit Localstorage	Y	Y	N
/private/var/mobile/Containers/Shared/AppGroup/<Apple_Files_GUID>/smartfolders.db	Apple Files	N	Y	N
/private/var/mobile/Containers/Shared/AppGroup/<Apple_Notes_GUID>/NoteStore.sqlite	iCloud Notes	N	Y	N
/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb	Contacts	N	Y	N
/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb	Contact Images	N	Y	N
/private/var/mobile/Library/Application Support/CloudDocs/session/db/client.db	Apple Files	N	N	N
/private/var/mobile/Library/Application Support/CloudDocs/session/db/server.db	Apple Files	N	N	N
/private/var/mobile/Library/Application Support/FileProvider/backup/backup_manifest.db	iCloud Documents details	N	N	N
/private/var/mobile/Library/Calendar/Calendar.sqlitedb	Calendar	N	Y	N
/private/var/mobile/Library/Calendar/Extras.db	Extras for Calendar	Y	Y	N
/private/var/mobile/Library/Calendar/Notifications.Calendar.Protected	Calendar entries	Y	N	N
/private/var/mobile/Library/CallHistoryDB/CallHistory.storedata	Call History	N	Y	N
/private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storedata	Call History Temporary storage (Before First Unlock)	Y	N	N
/private/var/mobile/Library/CallHistoryTransactions/<GUID>.log	Call log traces	N	N	N
/private/var/mobile/Library/com.apple.siri.inference/siriremembers.sqlite3	Siri Remembers	N	N	N
/private/var/mobile/Library/DuetExpertCenter/	User Notifications	N	N	N
/private/var/mobile/Library/Health/ActivitySharing/contacts2.dat	Apple Health Fitness Friends	N	N	N
/private/var/mobile/Library/Health/healthdb.sqlite	Apple Health	N	Y	N

Path	Description	BFU	Backup	Sysdiagnose
NETWORKS AND CONNECTIONS				
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db	Seen Bluetooth devices	N	Y	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db	Paired Bluetooth devices	Y	Y	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Preferences/com.apple.MobileBluetooth.devices.plist	Paired Bluetooth devices	N	Y	N
/private/var/db/dhcpclient/leases/	DHCP Leases	Y	N	N
/private/var/db/dhcpd_leases	DCHP Deamons Lease	N	N	N
/private/var/mobile/Library/Biome/sync/sync.db	Synced devices	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Devices.data	FindMy Devices	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/FamilyMembers.data	FindMy Family Members	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Items.data	FindMy Items (AirTags)	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Owner.data	FindMy Owner	N	N	N
/private/var/mobile/Library/DeviceRegistry.state/historySecureProperties.plist	Apple Watch information (also previously paired Apple Watch)	N	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/	Apple Watch data	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoAppRegistry/Applications/	Apple Watch Applications	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoMail/registry.sqlite	Apple Watch Mail application	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoPasses/nanopasses.sqlite3	Apple Watch Wallet Passes	N	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoPreferencesSync/Backup/Files/	Apple Watch Faces	Y	Y	N
/private/var/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db	Apple Watch Health data sync	N	Y	N
/private/var/mobile/Library/homed/datastore.sqlite	Apple Home information and devices	N	Y	N
/private/var/mobile/Library/NanoBackup/	Apple Watch information	Y	Y	N
/private/var/mobile/Library/NanoPreferencesSync/	Apple Watch information	Y	N	N
/private/var/mobile/Library/NanoTimeKit/	Apple Watch information	Y	N	N
/private/var/mobile/Library/Preferences/com.apple.carplay.plist	Apple CarPlay configuration	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.CarPlayApp.plist	Apple CarPlay configuration	Y	Y	N
/private/var/mobile/Library/Springboard/<GUID>-CarDisplay[Desired]IconState.plist	Apple CarPlay per car App Icon configuration	Y	Y	N
/private/var/mobile/Media/iTunesControl/iTunes/iTunesPrefs	List of computer where the device was connected to	Y	Y	N
/private/var/networkd/netusage.sqlite	Network data usage per App	N	N	N
/private/var/preferences/com.apple.networkextension.plist	Network Extension	Y	Y	N
/private/var/preferences/com.apple.wifi.known-networks.plist	Wi-Fi Network List	N	N	Y
/private/var/preferences/SystemConfiguration/com.apple.wifi.plist	Wi-Fi Network List (old format)	Y	Y	Y
/private/var/preferences/SystemConfiguration/com.apple.wifi-private-mac-networks.plist	Wi-Fi Network List	Y	Y	Y
/private/var/preferences/SystemConfiguration/preferences.plist	Wi-Fi, VPN, Certs and more	Y	Y	N
/private/var/root/Library/Application Support/com.apple.wifianalyticsd/DeviceAnalyticsModel.sqlite	Wi-Fi information	N	N	N
/private/var/root/Library/Application Support/WiFiNetworkStoreModel.sqlite	Wi-Fi information	N	N	N
/private/var/root/Library/Caches/com.apple.wifid/ThreeBars.sqlite	Wi-Fi information	N	N	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist	Wi-Fi ON/OFF	Y	Y	N
/private/var/wireless/Library/Databases/DataUsage.sqlite	Network data usage per App	N	Y	N
/private/var/wireless/Library/Preferences/com.apple.CommCenter.counts.plist	Data and Cellular network statistics	Y	Y	N

Android Cheatsheet

Partition	Path	File Format	Description
DEVICE INFORMATION			
System	/build.prop	TXT	Device information (version, patches, etc.)
Userdata	/data/com.google.android.gms/databases/constellation.db	SQLite	IMSI of last used SIM Card
Userdata	/data/com.google.android.gms/databases/ MdpSimBasedDatabase	SQLite	Sim card information
Userdata	/data/com.google.android.gms/shared_prefs/Checkin.xml	XML	Activity on device related to installed SIM (ICCID and Google Account included)
Userdata	/data/com.google.android.gsf/databases/gservices.db	SQLite	Fitness settings, network settings, other settings
Userdata	/property/persistent_properties	TXT	Timezone and local language
Userdata	/system/*.key	N/A	Files needed for password cracking
Userdata	/system/device_policies.xml	XML	Passcode requirements and policies. Syncing info may exist
Userdata	/system/locksettings.db	SQLite	Lock settings information
Userdata	/system/netpolicy.xml	XML	Timezone
Userdata	/system/users/<UserNumber>/settings_global.xml	ABX	Global settings
Userdata	/system/users/<UserNumber>/settings_secure.xml	ABX	Secure settings
Userdata	/system/users/<UserNumber>/settings_system.xml	ABX	System settings
Userdata	/user_de/<UserNumber>/com.android.providers.telephony/databases/telephony.db	SQLite	Sim card information
SYSTEM SETTINGS			
Userdata	/data/com.google.android.gms/shared_prefs/*	Various	Preference files
Userdata	/data/com.google.android.gsf/databases/googlesettings.db	SQLite	Google preferences – location, maps, wallet, etc. --!=true
Userdata	/data/com.google.android.gsf/databases/gservices.db	SQLite	Fitness settings, network settings, other settings
Userdata	/system/notification_policy.xml	ABX	Notifications settings
Userdata	/system/users/<UserNumber>/settings_global.xml	ABX	Global settings
Userdata	/system/users/<UserNumber>/settings_secure.xml	ABX	Secure Settings
Userdata	/system/users/<UserNumber>/settings_system.xml	ABX	System Settings
PASSWORDS AND ACCOUNT INFORMATION			
Userdata	/data/com.android.providers.contacts/databases/contacts2.db	SQLite	Login info
Userdata	/data/com.android.vending/shared_prefs/lastaccount.xml	XML	Last account used on Google PlayStore
Userdata	/data/com.google.android.gms/databases/google_account_history.db	SQLite	Google account history
Userdata	/data/com.google.android.gms/shared_prefs/BackupAccount.xml	XML	Backup account email address
Userdata	/data/com.google.android.gsf/databases/gservices.db	SQLite	Fitness settings, network settings, other settings
Userdata	/system/sync/accounts.xml	ABX	Account sync information
Userdata	/system/sync/accounts.xml	ABX	Syncing information
Userdata	/system/users/<UserNumber>.xml	ABX	Local user information and Last loggedin timestamp
Userdata	/system_ce/<UserNumber>/accounts_ce.db	SQLite	Accounts with credentials
Userdata	/system_de/<UserNumber>/accounts_de.db	SQLite	Accounts with creation timestamps
INSTALLED APPLICATIONS			
Userdata	/app/*	APK	APK files for installed applications
Userdata	/dalvik-cache	Various	.dex/.oat/.art files for installed applications
Usredata	/data/<Application_Sandbox>	Various	Application Data Files*
Userdata	/data/com.android.vending/databases/auto_update.db	SQLite	Packages set to auto update
Userdata	/data/com.android.vending/databases/frosting.db	SQLite	Tracks the installation and update of applications regardless of how they were installed
Userdata	/data/com.android.vending/databases/install_queue.db	SQLite	Installed packages
Userdata	/data/com.android.vending/databases/library.db	SQLite	Contains the library of applications for the Google user in use on the device.
Userdata	/data/com.android.vending/databases/localappstate.db	SQLite	Tracks applications installed on the device via the Google Play Store (not apps installed by other means)
Userdata	/data/com.android.vending/databases/suggestions.db	SQLite	Keywords searched on the Google Play Store
Userdata	/data/com.android.vending/databases/verify_apps.db	SQLite	Installed packages
Userdata	/data/com.android.vending/databases/xternal_referrer_status.db	SQLite	Installed applications. The information is not removed when an app is uninstalled
Userdata	/data/com.google.android.gms/databases/gass.db	SQLite	Tracks applications installed on the device, no matter how they were installed. It stores SHA-256 hash of the last APK.
Userdata	/misc_de/<UserNumber>/apexdata/com.android.permission/roles.xml	XML	List of applications set by default for certain functions in Android
Userdata	/misc_de/<UserNumber>/apexdata/com.android.permission/runtime-permissions.xml	XML	Dangerous permissions information (for each package and each permission, granted true/false)

*Important Skill: Logs

- The bedrock and starting point of most security investigations begins with any available logs.
- Private vs Public

Native Logs

Understanding where logs exist on various endpoints is vitally important

- **Windows Logs**
  - %System32%\winevt\Logs
- **Linux Logs**
  - /var/log/syslog
- **Server Logs**
  - %SystemDrive%\inetpub\logs\LogFiles
- **Application Logs**
  - Depends on applications, some may stored in centralized management

SQL Basics Skills

- Understand “Structured Query Language” (SQL) to parsed browser history artifacts and other *.DB

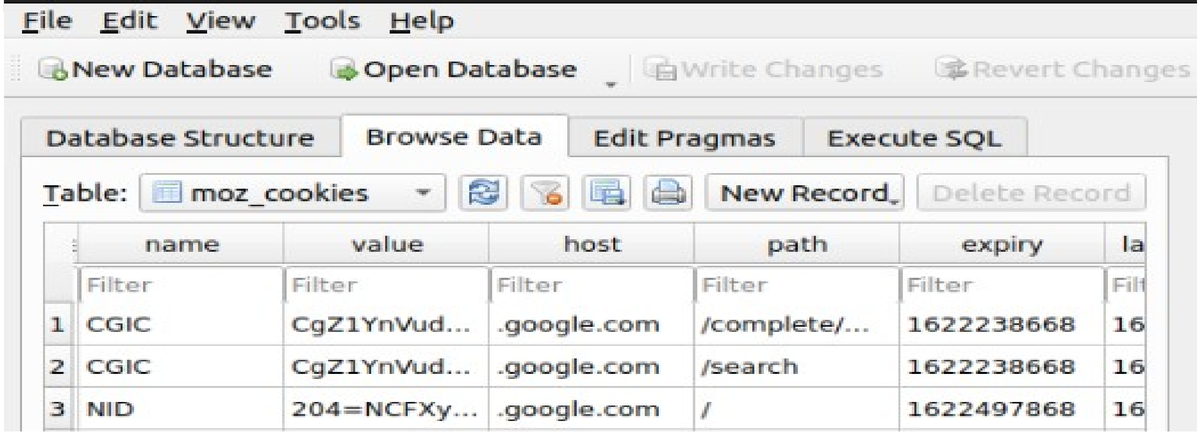


Table: moz_cookies

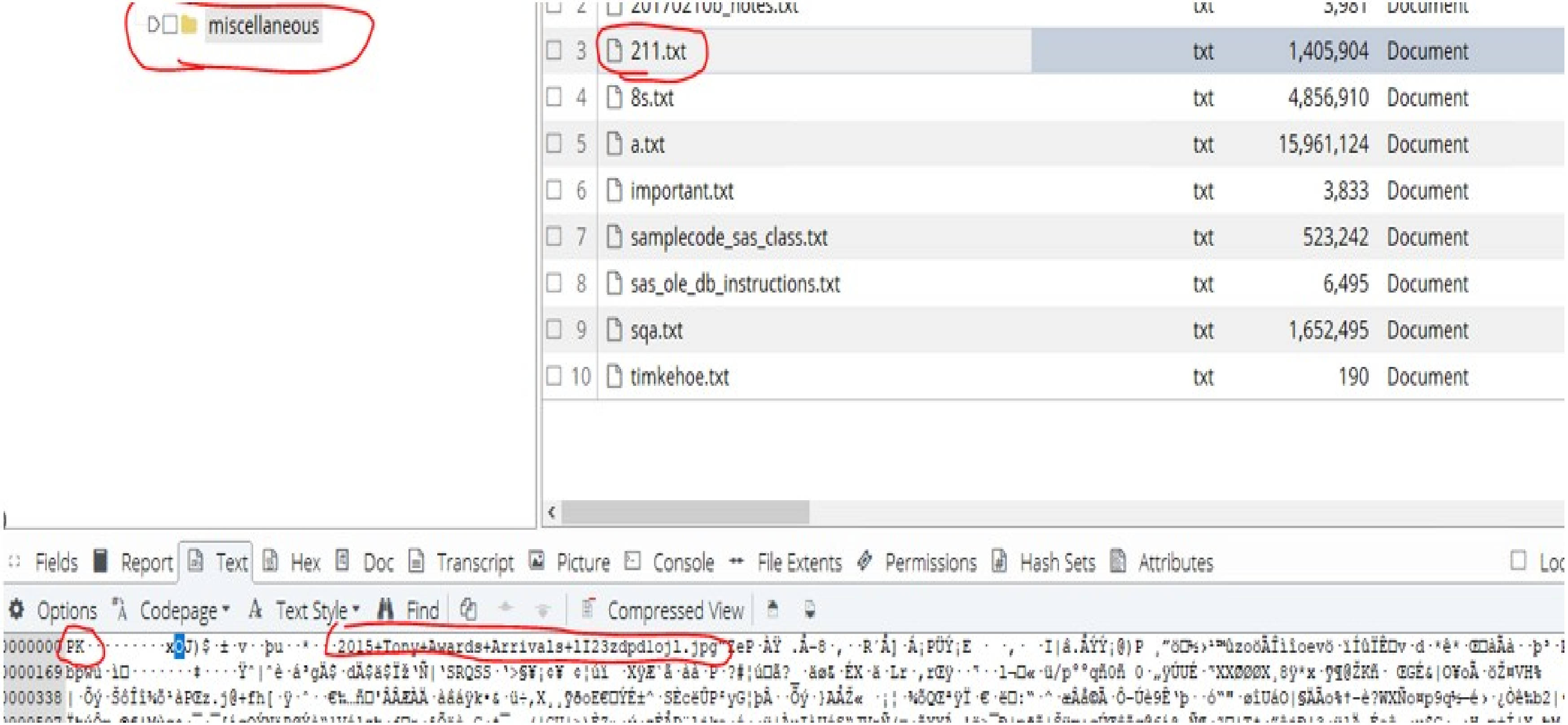
	name	value	host	path	expiry	la
	Filter	Filter	Filter	Filter	Filter	Filt
1	CGIC	CgZ1YnVud...	.google.com	/complete/...	1622238668	16
2	CGIC	CgZ1YnVud...	.google.com	/search	1622238668	16
3	NID	204=NCFXy...	.google.com	/	1622497868	16

- Free online training
  - https://www.sqlcourse.com/beginner-course/
  - https://www.sqlcourse.com/advanced-course/

File Type Identification Skills

- **Understand file signatures, file headers, or whatever you prefer to call them…**
  - Because file extensions can be altered or removed
- **https://www.garykessler.net/library/file_sigs.html**

File Type Case Study



		Name	Type	Size	Kind
□	2	20170210b_notes.txt	txt	3,981	Document
□	3	211.txt	txt	1,405,904	Document
□	4	8s.txt	txt	4,856,910	Document
□	5	a.txt	txt	15,961,124	Document
□	6	important.txt	txt	3,833	Document
□	7	samplecode_sas_class.txt	txt	523,242	Document
□	8	sas_ole_db_instructions.txt	txt	6,495	Document
□	9	sqa.txt	txt	1,652,495	Document
□	10	timkehoe.txt	txt	190	Document

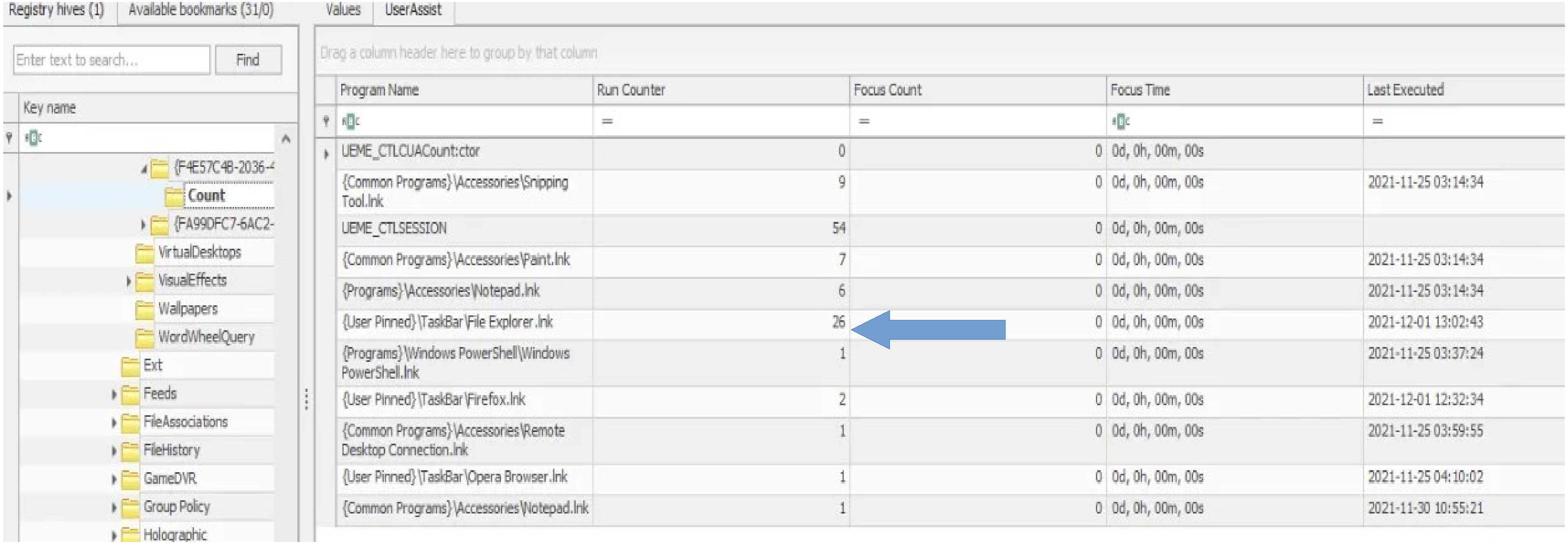
```
0000000 PK·········xOJ)$·±·v··þu··*··2015+Tony+Awards+Arrivals+1I23zdpdloj1.jpg"ZeP·ÀŸ .Å-8·,··R`Å]·Á¡PÜÝ¡E··,··I|â.ÅÝÝ¡@)P ,"öÞ½›¹™ûzoöÂÎìîoevö·ìÎûÎÊÞv·d·*è*·ŒÞåÀà··þ³·
0000169 bpwü·ìÞ·······‡····Ÿ^|^è·á³gÂ$·dÃ$ä$Îž'Ñ|'SRQSS·'>§¥¡¢¥ ¢¦úí ·XÿÆ'å·àà·P·?‡¦úÞå?_·äøš·ÉX·ä·Lr·,rŒÿ··¨··1¬Þ«·û/p°°qñOñ 0·„ÿÚÚÉ·¯XXØØØX,8ÿ*x·ÿ¶@ŽKñ· ŒGÉ&|O¥oÃ·öŽ¤VH$
0000338 |·Õý·ŠôÎî¾õ¹àPŒz.j@+fh[·ÿ·^··€ħ…ñÞ'ÂÅÆÀÀ·àáâýk•&·ü÷,X,,ƒðoE€ÞÝÉ±^·SÈcéÛP²yG¦þÅ··Õý·}AÅŽ«·¦¦·¾õQŒ²ÿÏ·€·€Þ:"·^·æÅå©Ã·Ó-Üè9Ë'þ··ó""·øîÙáO|§ÃÂo¾†-è?WXÑo¤p9q½—é›·¿Öè‰b2|
```

Identify File Execution

- Understand how to know if a file executed on a Windows endpoint
  - Some Examples for the registry key:
    - **UserAssist**
    - **RecentApps**
    - **ShimCache**
    - **CurrentVersion**
    - **Prefetch - %windir%\Prefetch**

File Execution Case Study

- **UserAssist**
  - How many times was the File Explorer launched? (26)



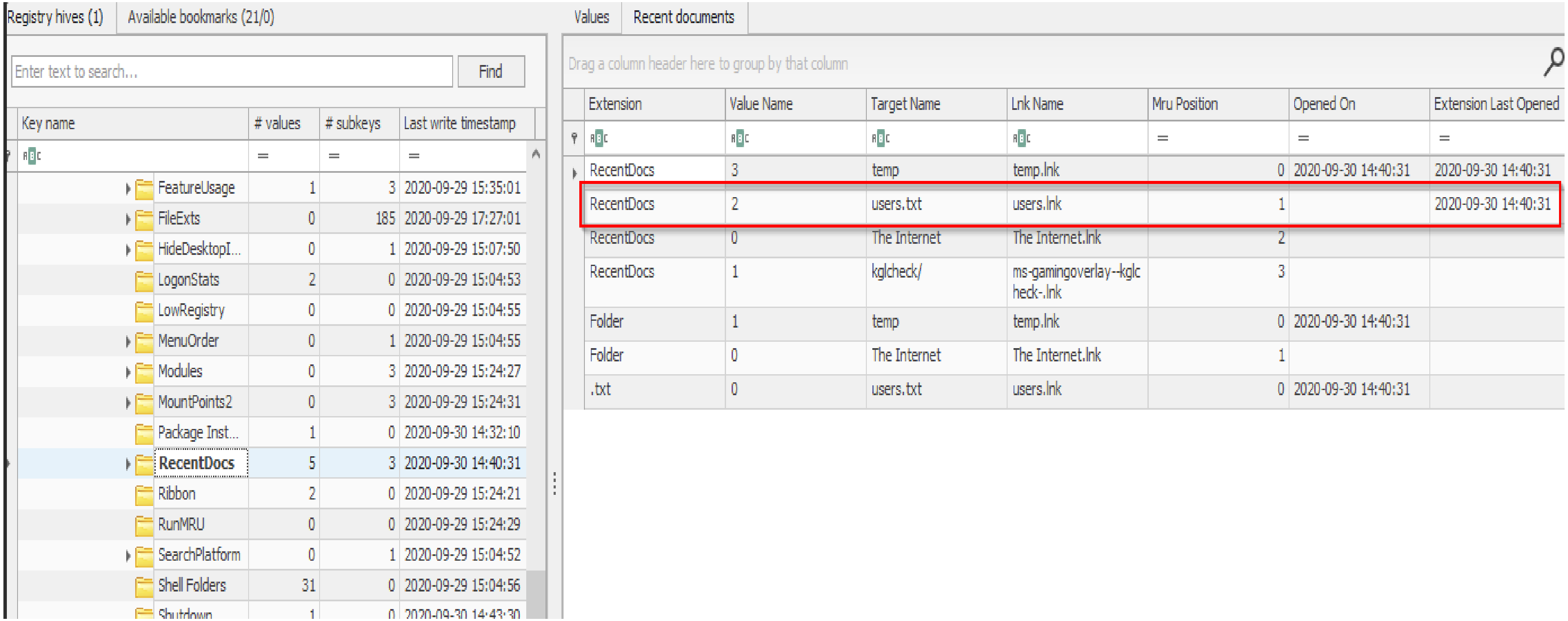
Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Snipping Tool.lnk	9	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
UEME_CTLSESSION	54	0	0d, 0h, 00m, 00s	
{Common Programs}\Accessories\Paint.lnk	7	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
{Programs}\Accessories\Notepad.lnk	6	0	0d, 0h, 00m, 00s	2021-11-25 03:14:34
{User Pinned}\TaskBar\File Explorer.lnk	26	0	0d, 0h, 00m, 00s	2021-12-01 13:02:43
{Programs}\Windows PowerShell\Windows PowerShell.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 03:37:24
{User Pinned}\TaskBar\Firefox.lnk	2	0	0d, 0h, 00m, 00s	2021-12-01 12:32:34
{Common Programs}\Accessories\Remote Desktop Connection.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 03:59:55
{User Pinned}\TaskBar\Opera Browser.lnk	1	0	0d, 0h, 00m, 00s	2021-11-25 04:10:02
{Common Programs}\Accessories\Notepad.lnk	1	0	0d, 0h, 00m, 00s	2021-11-30 10:55:21

Identify File Activity Skill

- Understand how to know if a file was accessed.
  - This activity is tracked under the following registries below:
    - Jump Lists
    - RecentDocs
    - LastVisitedMRU – last path file opened\executed
    - OpenedSavedPidMRU
    - LNK files
    - ShellBags
    - etc

File Activity Case Study

- RecentDocs


Registry hives (1)
Available bookmarks (21/0)
Enter text to search...
Find
Values
Recent documents
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write timestamp
FeatureUsage	1	3	2020-09-29 15:35:01
FileExts	0	185	2020-09-29 17:27:01
HideDesktopI...	0	1	2020-09-29 15:07:50
LogonStats	2	0	2020-09-29 15:04:53
LowRegistry	0	0	2020-09-29 15:04:55
MenuOrder	0	1	2020-09-29 15:04:55
Modules	0	3	2020-09-29 15:24:27
MountPoints2	0	3	2020-09-29 15:24:31
Package Inst...	1	0	2020-09-30 14:32:10
RecentDocs	5	3	2020-09-30 14:40:31
Ribbon	2	0	2020-09-29 15:24:21
RunMRU	0	0	2020-09-29 15:24:29
SearchPlatform	0	1	2020-09-29 15:04:52
Shell Folders	31	0	2020-09-29 15:04:56
Shutdown	1	0	2020-09-30 14:43:30

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	3	temp	temp.lnk	0	2020-09-30 14:40:31	2020-09-30 14:40:31
RecentDocs	2	users.txt	users.lnk	1		2020-09-30 14:40:31
RecentDocs	0	The Internet	The Internet.lnk	2		
RecentDocs	1	kglcheck/	ms-gamingoverlay--kglcheck-.lnk	3		
Folder	1	temp	temp.lnk	0	2020-09-30 14:40:31	
Folder	0	The Internet	The Internet.lnk	1		
.txt	0	users.txt	users.lnk	0	2020-09-30 14:40:31	

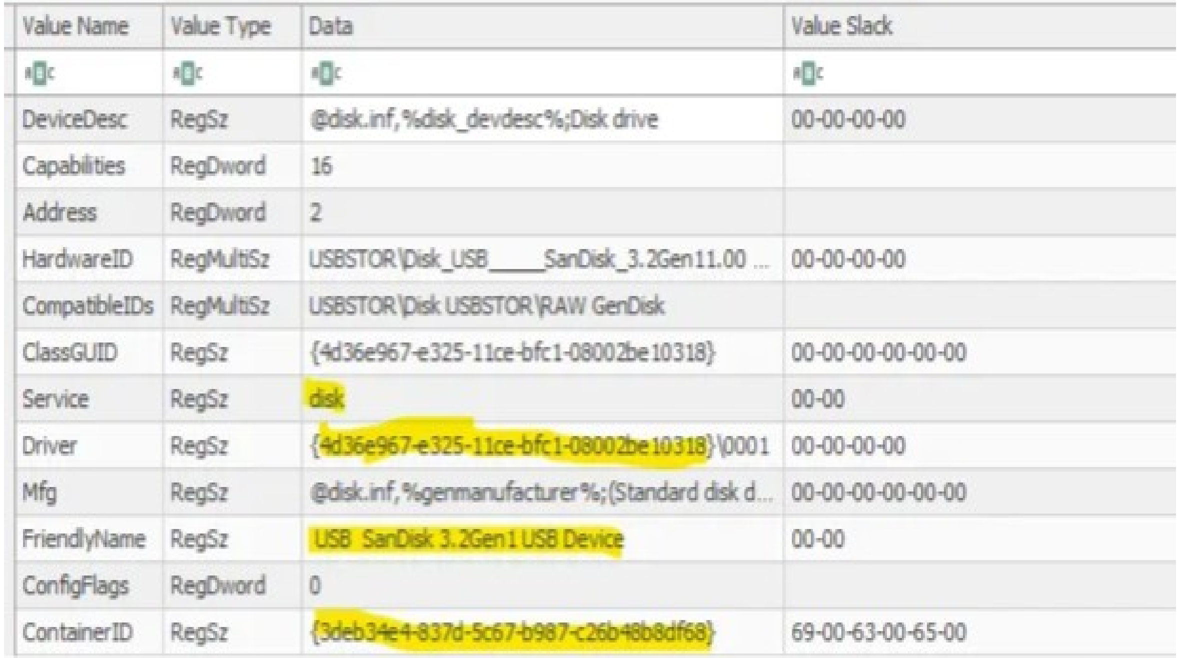
Identify USB Activity Skill

- **Understand how to know if a USB was connected.**
  - **The majority of USB-related artifacts are located within the Windows Registry**
    - SYSTEM\CurrentControlSet\Enum\USBSTOR
    - SYSTEM**MountedDevices**
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
  - **Windows Event Logs:**
    - System event logs may contain entries related to USB device insertions and removals.
    - Event Viewer path: Applications and Services Logs\Microsoft\Windows\DriverFrameworks-UserMode\Operational

USB Activity Example

- **USBSTOR:**
  - SYSTEM\CurrentControlSet\Enum\USBSTOR

- **Things to Record:**
  - Device S/N:
  - Vendor:
  - Product:
  - Service:
  - Container Id:



Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive	00-00-00-00
Capabilities	RegDword	16	
Address	RegDword	2	
HardwareID	RegMultiSz	USBSTOR\Disk_USB_____SanDisk_3.2Gen11.00 ...	00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk	
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	00-00-00-00-00-00
Service	RegSz	disk	00-00
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk d...	00-00-00-00-00-00
FriendlyName	RegSz	USB SanDisk 3.2Gen1 USB Device	00-00
ConfigFlags	RegDword	0	
ContainerID	RegSz	{3deb34e4-837d-5c67-b987-c26b48b8df68}	69-00-63-00-65-00

Understand Order of Volatile

- **Collect and Protect information relating to an incident**
  - Many different data source and protection mechanisms
- **RFC 3227 – Guidelines for Evidence Collection and Archiving**
  - A good set of best practices
- **How Long Does data stick around?**
  - Some media is much more volatile than others
  - Gather data in order from most to less
    - registers, cache
    - routing table, arp cache, process table, kernel statistics, memory
    - temporary file systems
    - disk
    - remote logging and monitoring data that is relevant to the system in question
    - physical configuration, network topology
    - archival media

Forensics Tools for skill building

- **Many tools can be used to perform data analysis on different Operating Systems.**
- **Forensic toolkit for Win\Linux**
  - Kali, Helix, DEFT, Autopsy Sleuth-kit, SIFT
  - FTK imager, Nirsoft
  - Velociraptor, Kape
- **Mobile Forensics**
  - SAFT, Autopsy, Belkasoft
  - iLEAP

Ways to build Forensic skills

- **Follow Cyber Security Linkedin group free training and webinars.**
  - CYBER SECURITY FORUM INITIATIVE – CSFI
  - Forensic Focus
  - Belkasoft
  - Sleuth Kit Labs
- **Follow and watch YouTube Digital Forensics Channel**
  - TEDx Talks
  - SANS
  - Google Career Certificates
  - Others
- **Check out ENISA**
  - https://www.enisa.europa.eu/

Just Some of the Challenges

- Rapidly changing technology and Data volumes
- System & Application update
- Mental health
- Ongoing education
- Unsupported devices
- Encryption\Security Features

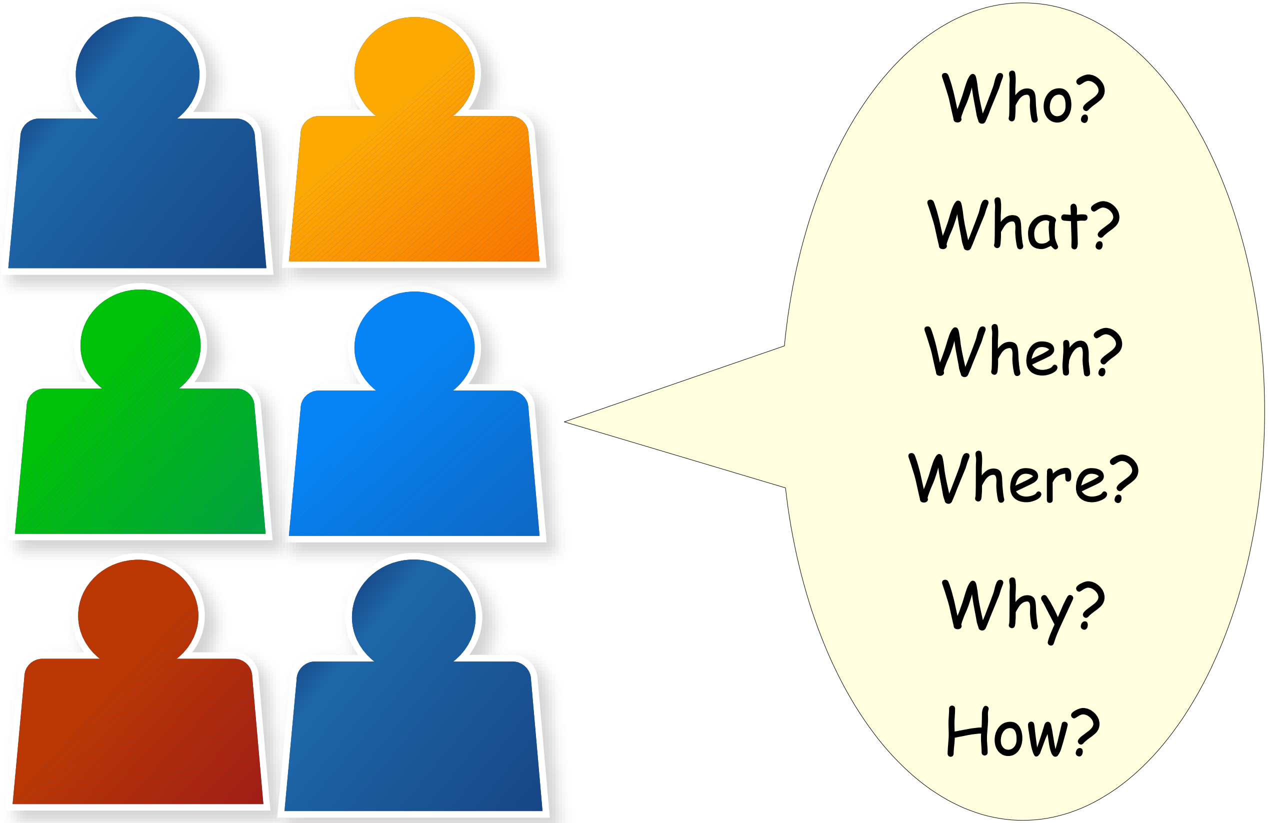
Certifications

- **Some well-known forensic certifications include the following:**
  - **CISSP** – Certified Information Systems Security Professional
  - **CCE** – Certified Computer Examiner
  - **CFCE** – Certified Forensic Computer Examiner
  - **GIAC** – Certified Forensic Analyst (GCFA)
  - **CompTIA A+, Network+, Security+**

Salary & Benefits

- **The starting salary for a computer forensics professional depends on various factors.**
  - Whether you’re employed in the public or private sector.
  - Degree (s) vs Certification (s)
  - # of years of experience
  - Location

Questions



Who?

What?

When?

Where?

Why?

How?

Thank you for Attending!

Tuan Phan

*****https://github.com/phanrensics/slides*****