Computer Forensic Lifecycle (common PC/Laptop)

1. **Preparation**
    a. Preparation steps
        i. Test and familiarize yourself with software tools
        ii. Prepare hard drives
            1. Wipe & verify
            2. Partitioning
                a. Filesystem type
            3. Load tools
        iii. Prepare flash drives
            1. Wipe & verify
            2. Partitioning
                a. Filesystem type
            3. Load tools
    b. Initial response kit
        i. Necessary hardware
            1. Prepared flash drive(s)
            2. Prepared hard drive(s)
            3. Hand tools
        ii. Necessary software
            1. RAM collection software
            2. Encryption detection software
            3. Imaging software
        iii. Other necessary equipment
            1. Forms (CoC, computer worksheet)
            2. Notepad
            3. Bags, tape, labels, pens
            4. Camera/Video

2. **Identify, Triage, Collect and Document**

    a. Initial response considerations
        i. Safety
        ii. Safeguarding digital evidence from further tampering
        iii. Urgency

    b. Triaging Live computers
        i. Initial triage
            1. Deletion or other potentially destructive action in progress?
                a. Stop process vs. shutting down computer
            2. If circumstances dictate, disconnecting physical network connection
                a. Necessary to collect minimal information prior to disconnection?
                b. Disconnect physical network connection
                    i. Hardware wireless switch (laptop)
        ii. Unlocked Screen
            1. Wireless status/disconnect required?
            2. Determine level of access
                a. Administrator access
                    i. Collection of volatile data
                        1. Follow order of volatility
                            a. RAM collection
                            b. Other volatile Data
                                i. Comprehensive networking information
                                ii. Running applications
                                iii. Date & time
                            c. Detecting encrypted volumes

i. Logical imaging
ii. Obtain Bitlocker recovery key
2. Shutdown system
b. Non-administrator access
i. Collection of volatile data
1. Follow order of volatility
a. Other volatile data
i. Comprehensive networking information
ii. Running applications
iii. Date & time
b. Detecting encrypted volumes
i. Logical imaging
iii. Locked Screen
1. Shutdown system
a. Pulling plug vs. shutdown process
c. Collection of digital media
i. Marking/labeling
d. Documentation
i. CoC
ii. Notes

3. **Imaging Process**
    a. Interface considerations – Available adapters and connectors
        1. USB
        2. SCSI
        3. PATA
        4. SATA
        5. SAS
        6. ZIFF

    b. Hardware-based imaging devices
        i. Storage considerations
            1. Pre-prepared HD (wiped)
            2. Drive capacity
        ii. Tableau
            1. Native .E01 support
        iii. Weibetech
        iv. Logicube

    c. Software Imaging
        i. Storage considerations
            1. Pre-prepared HD (wiped)
            2. Drive capacity
        ii. Hardware write-blockers
            1. Tableau
            2. Weibetech
            3. Others
        iii. Software write-blockers
            1. EnCase Fastbloc SE
            2. Registry hack

iv. No write blocker
    1. Linux / Unix / OSX

d. Verification Process
    i. Hash verification

4. Analysis Process

a. Pre-Analysis preparation
    i. Root Case Folder
        1. Location
        2. Naming convention
        3. Case folder subcomponents
            a. Evidence files
            b. Export
            c. Temp
            d. Index

b. Pre-Analysis Processing
    i. Identification of all archives, encrypted volumes, virtual machines.
        1. Virtual mounting

    ii. Hash Analysis
        1. Good vs. bad hashes (Known vs. Unknown)
        2. Generating hash values for each file
        3. Comparing hash sets
        4. Filtering out identified files

    iii. File Signature Analysis

    iv. Keyword indexing (optional)

c. Case-Specific Analysis Techniques (common techniques)
    i. RAM Analysis (if applicable)
        1. Strings
        2. Redline
        3. HBGary Responder

    ii. Keyword Searching
        1. Live searching
        2. Index Searching
        3. Unicode
        4. GREP

    iii. Internet History Analysis
        1. IE
            a. Internet history
            b. Favorites
            c. Zone identifier files
            d. Configuration settings

        2. Firefox
            a. Internet history
            b. Favorites
            c. Configuration settings

        3. Chrome
            a. Internet history
            b. Favorites
            c. Configuration settings

4. Safari
    a. Internet history
    b. Favorites
    c. Configuration setting

5. 3rd party tools
    a. Netanalysis
    b. Web Historian

iv. Email Analysis
1. Client based
    a. Outlook
    b. Outlook Express
    c. Thunderbird
2. Web based
    a. Gmail
    b. Hotmail
    c. Yahoo

v. Windows Event logs
1. Location
2. Types
3. Format
    a. XP vs. Vista / 7/ 8
4. 3rd party tools
    a. Splunk
    b. Highlighter

vi. Social Media Analysis
1. Twitter

2. Facebook
3. Google+

vii. Instant Messaging
1. Gtalk
2. Yahoo
3. Live / Communicator / Lync

viii. User Profile Analysis (recent docs, LNK, etc)
1. Desktop
2. Downloads
3. Documents
4. Videos
5. Photos

ix. Registry Analysis
1. Global
    a. User accounts / SIDS
    b. Installed applications
    c. Passwords
2. User Specific
    a. Protected Storage Passwords
    b. UserAssist
    c. MRU / Recently opened files
    d. Background Image
3. 3rd party tools
    a. regripper
    b. regdecoder
    c. WRR (mitec)

x. USB Device Analysis

1. XP
    a. Registry
        i. Mounted Devices
        ii. USBSTOR
    b. setupapi.log
2. Vista / 7 / 8
    a. Registry
        i. Mounted Devices
        ii. USBSTOR
    b. setupapi.dev.log & setupapi.app.log

xi. Recycle Bin Analysis
1. SID mapping

xii. System Restore Points / Volume Shadow Service (VSS) analysis
1. XP systems
    a. 3rd party tools
        i. Mandiant Restore Point analyzer
2. Vista / 7/ 8
    a. VSS Analysis
    b. 3rd party tools
        i. ShadowExplorer
        ii. FAU dd (Garner)

xiii. Peer-to-Peer (P2P) Analysis
1. Limewire
2. Gigatribe
3. uTorrent

xiv. Cloud Based Applications

1. Dropbox
2. Microsoft Live mesh
3. Google drive

xv. Basic Data Carving
    1. pagefile.sys
    2. hiberfil.sys
    3. Unallocated Space
    4. Identifying headers & footers
        a. Base64
        b. Internet History
    5. 3rd party tools
        a. Internet Evidence Finder (IEF)

xvi. Unused Disk areas
    1. Deleted partitions

xvii. General Intelligence gathering
    1. Collection of email addresses
    2. Collection of phone numbers

5. Report Writing

a. Baseline & Case specific information
    i. Request
    ii. Findings
        1. Drive Info
            a. Physical size (label)
            b. Physical size (BIOS)
            c. Logical size
                i. Logical partitions

        d. Unused disk space
    2. OS Information
        a. Type
        b. Version
        c. Patch level / hotfixes
        d. Install date
        e. Registered Name / Organization
    3. Case specific findings
iii. Summary
iv. Recommendations

b. Timeline of events