Non-Forensic, Defensible Collection Checklist

Client/Matter Name: _____

Client/Matter #: _____

Custodian Name: _____

Collection Date: _____

Attorney name: _____

Analyst name: _____

- ☐ Based on collection plan, determine script to run to perform collection
- ☐ Log observations regarding custodian device
  - Manufacturer
  - Model
  - Serial Number
  - Date, time and timezone
  - Identify users who accessed device in addition to custodian
- ☐ Cold boot device allowing minimum one-minute RAM decay
- ☐ Have custodian Login as self, administrator Login as custodian, or Login as custodian yourself
- ☐ Connect collection drive and confirm operation and recognition by OS
- ☐ Run Windows Task manager and note processes running
  - Terminate all processes which may lock target files or otherwise interfere with collection
- ☐ Note in collection log all processes running at start of collection
- ☐ Perform collection per established procedures
- ☐ Monitor collection process for speed against collection plan timeline and errors logged
- ☐ Finish collection procedure as all files are collected
- ☐ Review collection log and determine if any files failed to copy
- ☐ Make reasonable efforts to retrieve files that failed to copy
- ☐ Finalize collection; update log notes; clear media of collection software files
- ☐ Stop and disconnect collection drive
- ☐ Cold boot target device
- ☐ Return to custodian use