PEER REVIEW CHECKLIST - MOBILE FORENSICS

Scope:

- ☐ Authority: All items analyzed were done so with appropriate legal authority such as warrant or consent.
- ☐ Online / Cloud Data: Any cloud storage sources analyzed were done so in accordance with rules, laws, and regulations that pertain to the investigation to include jurisdiction and organization policies.
- ☐ Analysis Scope: The analysis completed solely focused on topics and evidence allowed under the authority utilized to conduct the investigation.
- ☐ Reportable Items: All information of a required reportable nature discovered during analysis was provided to stakeholder for further instruction
- ☐ Response: The analysis responds to the investigative question(s) asked.
- ☐ Writing: The analysis is free of generalizations and opinions. If examiner comments are included, they are labeled.

Acquisition Tools:

- ☐ Acquisition Tool Verification: The examiner clearly documented the dates and described the method of last known tool(s) verification.
- ☐ Acquisition Tool Validation: The examiner clearly documented the dates and described the method of last known tool(s) validation.
- ☐ Non-Forensic Tool(s): The examiner demonstrated that integrity of data was maintained when using non-forensic tools for analysis functions. For example, if applying the WAL to an SQLite database to facilitate analysis, that it was done to a copy of the files and not the gold forensic image.
- ☐ Acquisition Method & Forensic Tool(s): The examiner conducted the most comprehensive acquisition possible with the forensic tool(s) available. Were multiple acquisition types utilized? If multiple types of acquisitions were created, did they follow best practices in terms of acquisition order?
- ☐ Acquisition Data Hashing: The examiner documented how the acquisition data was hashed and the results were verified.
- ☐ Errors/issues: The examiner documented any known errors that occurred during the parsing process and any corrective actions taken.

Analysis Tools:

- ☐ Parsing Tool Verification: The examiner clearly documented the dates and described the method of last known tool(s) verification.
- ☐ Parsing Tool Validation: The examiner clearly documented the dates and described the method of last known tool(s) validation.
- ☐ Application Parsing: The examiner documented how the application data was parsed (Commercial tool, other).
- ☐ Analysis Forensic Tool(s): The examiner included all forensic tools utilized during the analysis process to include the software version in the report.
- ☐ Availability of tools to support parsing of artifacts was researched.
- ☐ All applicable available parsing utilities were run against the source data.
- ☐ Errors/issues: The examiner documented any known errors that occurred during the parsing process and any corrective actions taken.

Analysis Process:

- ☐ Unsupported Apps: Installed applications compared to parsed applications to discover potential apps of interest and pertinence to scope.
- ☐ Deleted Apps: Applications that were deleted have been compared to parsed applications and reviewed as related to the inquiry.
- ☐ Operating System Artifacts: User artifacts have been correlated to system artifacts to support actions and application usage. Example would be demonstrating an application was in the foreground using operating system artifacts at a time correlating to user actions in the application based on parsed application data.
- ☐ Verification/Validation of Supported Artifacts: Artifacts parsed by tools that are relevant to investigation have been verified with either known exemplar data parsing or manual review of source data to ensure pertinent data was properly decoded.
- ☐ Geolocation artifacts: Geolocation artifacts validated for accuracy, precision, and determination if the location was visited, subject of an inquiry, or information shared from another device, application, or user.
- ☐ Timelines and timestamps: Timestamps and timelines referenced are accurate in terms of understanding if a particular timestamp was recorded and referenced based on the local time of the device, Coordinated Universal Time (UTC), and the meaning of the timestamp (i.e. the time a picture was taken vs. the time it was written to cloud storage).

Reviewer Signature _____

Date _____

Case Reference _____