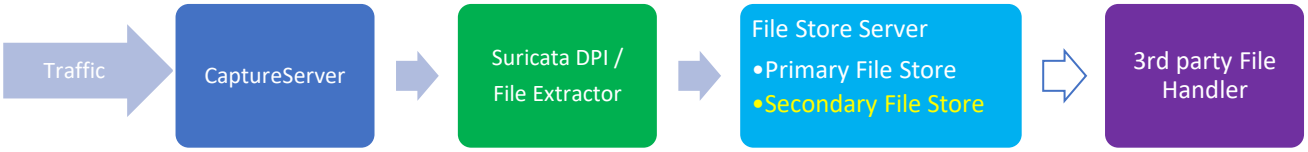
SentryWire
PACKET CAPTURE PLATFORM

Brief overview of the File Carving Workflow with Secondary File Store and alerts
(09.27.21 – will be added to v1.9 of the main workflow document)



Suricata File Extractor generates files and passes them on to File Store Server.

File Store Server:

1. Duplicate files (with in a day) are **not** saved/forwarded.
2. Files corresponding to excluded domains, ipaddresses, file types are **not** saved/forwarded.
3. If FC Primary File Store is full, generate Severity 1 **Primary File Store Full** Alert, move 25% current files into FC Secondary File Store If the Secondary File Store has space. The alert helps decide if the File Store is too small, or if the 3rd party File Handler is too slow or the network connectivity is bad. If the Secondary File Store is also Full, generate Severity 1 **Secondary File Store Full Alert** and delete 25% of the Secondary File Store. This alert will include the names of each unsent file deleted.
4. Each file is sent with its associated communityid or 4-tuple and hostname to Reversing Labs using their REST API POST call. The additional info appended to the carved file name will be used for mapping the results back to the flow/pcaps that produced the file.
5. If successful, it is logged as Severity 3(Informational) **Inspected Carved File Deleted** event and the file is deleted from the File Store.
6. If not successful, the FC server retries until CacheRetentionTime(minutes), then moves the file to the Secondary File Store.
7. If Off-peak hours and FC Secondary File Store is not empty, retry sending each file to the 3rd Party File Handler (as described in steps 4 and 5 above). If not successful, delete the file and generate Severity 1 **Uninspected Carved File Deleted** Alert.
8. Rinse, Repeat...