**1.** Normalize emails with known format (procmail + python script)

**1.1** Extract IP (or username, if from Splunk report) and timestamp from each report

**1.2** Combine multiple reports for a given IP address/username

**1.3** Add metadata (e.g. Source type, Report type) to each

**2.** Send one email per IP/username to email gateway for ticketing system (DMCA complaints go to email gateway directly without preprocessing above)

**3.** In ticketing system (RTIR – Request Tracker for Incident Response), use automation hook upon Incident Report creation to extract ticket details:

**3.1** If DMCA complaint, parse ACNS fields to extract IP & timestamp and set DMCA-specific fields

**3.2** Otherwise, ticketing system hands off just IP & timestamp

**4.** Use automation hook (written in perl) to enrich:

**4.1** Map IP address to department; use business rules to map department to email address of local support provider

**4.2** Look up IP address in database of critical/sensitive hosts; set flag as needed

**4.3** If IP address is in wireless network:

4.3.1 Look up associated username in attribution system (uses DHCP, RADIUS accounting, and EAP authentication logs in Splunk + logic to identify user associated with IP and timestamp, queried using API); and

4.3.2 If username was identified, look up affiliation and department in people database

4.3.3 Use business rules to map username, affiliation, and department to email address of local support provider

**4.4** Return aforementioned database lookups and derived data to ticketing system, which adds it to the Incident Report

**5.** Ticketing system checks data in enriched Incident Report - if suitable for automated resolution (perl), it:

* 1. Creates Incident (indicates a processed Incident Report that should be counted in our metrics)
  2. Creates Investigation (child of Incident, used for communication with local support providers)
  3. Sends email to local support provider (or to student directly, if DMCA)
  4. Resolves the Incident, Incident Report, and Investigation

**6.** Local Support Provider follows up on the report