`apt` 파이프라인 워크플로우

```
Step 1: 해시 목록 준비 (Prepare Hash List)
# Amadey 태그로 100개 샘플 해시 수집
bash scripts/apt_docker.sh python3 malwarebazaar_hunt.py --tag amadey --limit 100

Step 2: 악성코드 샘플 다운로드 (Download Malware Samples)
# 해시 목록 기반으로 파일 다운로드 및 압축 해제
bash scripts/apt_docker.sh python3 malwarebazaar_download.py --file /data/amadey_100_hashes.txt

Step 3: 메모리 덤프 다운로드 (Download Memory Dumps)
# Hybrid-Analysis에서 메모리 덤프 다운로드
bash scripts/apt_docker.sh bash fetch_memory_dump.sh --sha256-list /data/amadey_100_hashes.txt

Step 4: YARA 스캔 및 결과 집계 (Scan with YARA & Aggregate Results)
# 다운로드된 파일 스캔
bash scripts/apt_docker.sh python3 scripts/yara_eval.py --rules ... --target /data/unzip_amd_100

# 메모리 덤프 스캔 (압축 해제 후)
bash scripts/apt_docker.sh python3 scripts/yara_eval.py --rules ... --target /data/ha_dumps_unz
```

모든 과정은 스크립트화되어 있으며, Docker 안에서 안전하고 반복적으로 실행할 수 있습니다.