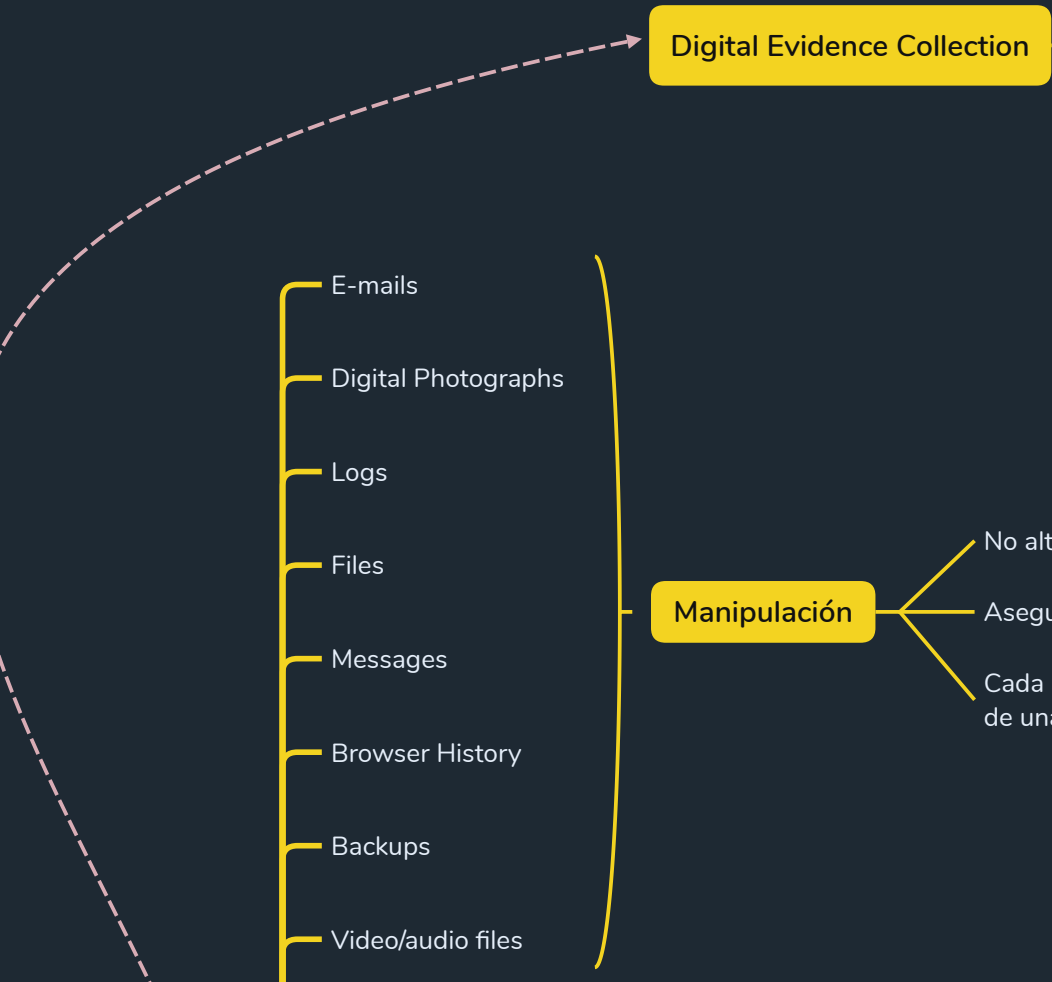


Digital Forensics

- Proceso
- 1. Identification
 - 2. Preservation
 - 3. Collection
 - 4. Analysis
 - 5. Reporting

- Conceptos
- Binary
 - Base64
 - Hexadecimal
 - Octal
 - ASCII



METADATA

Windows:

Propiedades del archivo

Linux:

```
#ls -lisp <file>
#stat <file>
#exiftool
```

FILE CARVING

```
#etcc/scalpel/scalpel.conf
#scalpel 30 -o output <disk image file>
```

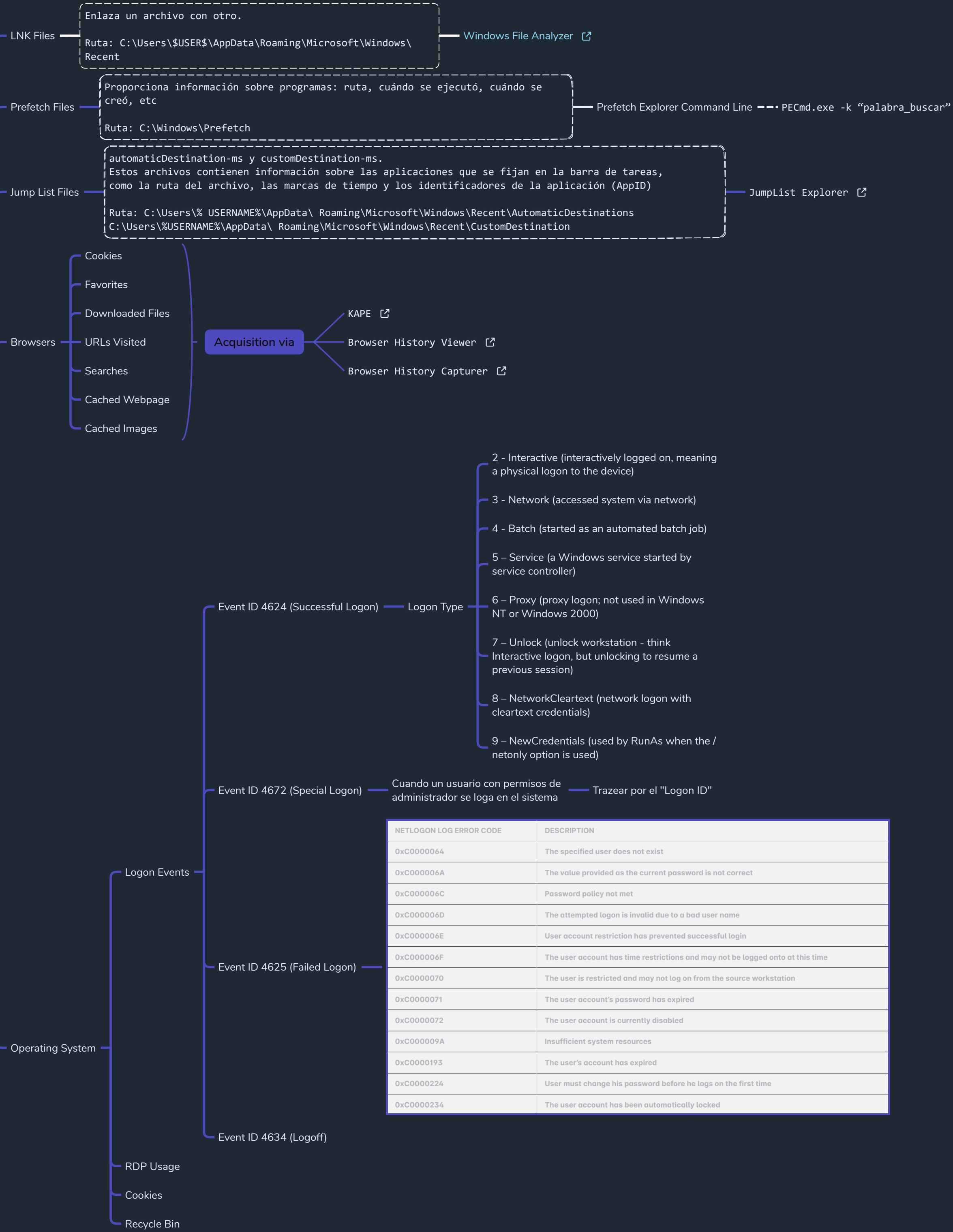
Order of Volatility

- 1 Registers & Cache
- 2 Memory
- 3 Disk
- 4 Remote Logging and Monitoring Data
- 5 Physical Configuration, Network Topology, Archival Media

Metadata and File Carving

Windows Investigations

Linux Investigations



Analysis

