NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The NSRL and Video Games

Why I Get to Buy Video Games at the Office

FORENSICS @ NIST

#NISTForensics

Disclaimer

Trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

The National Software Reference Library (NSRL)

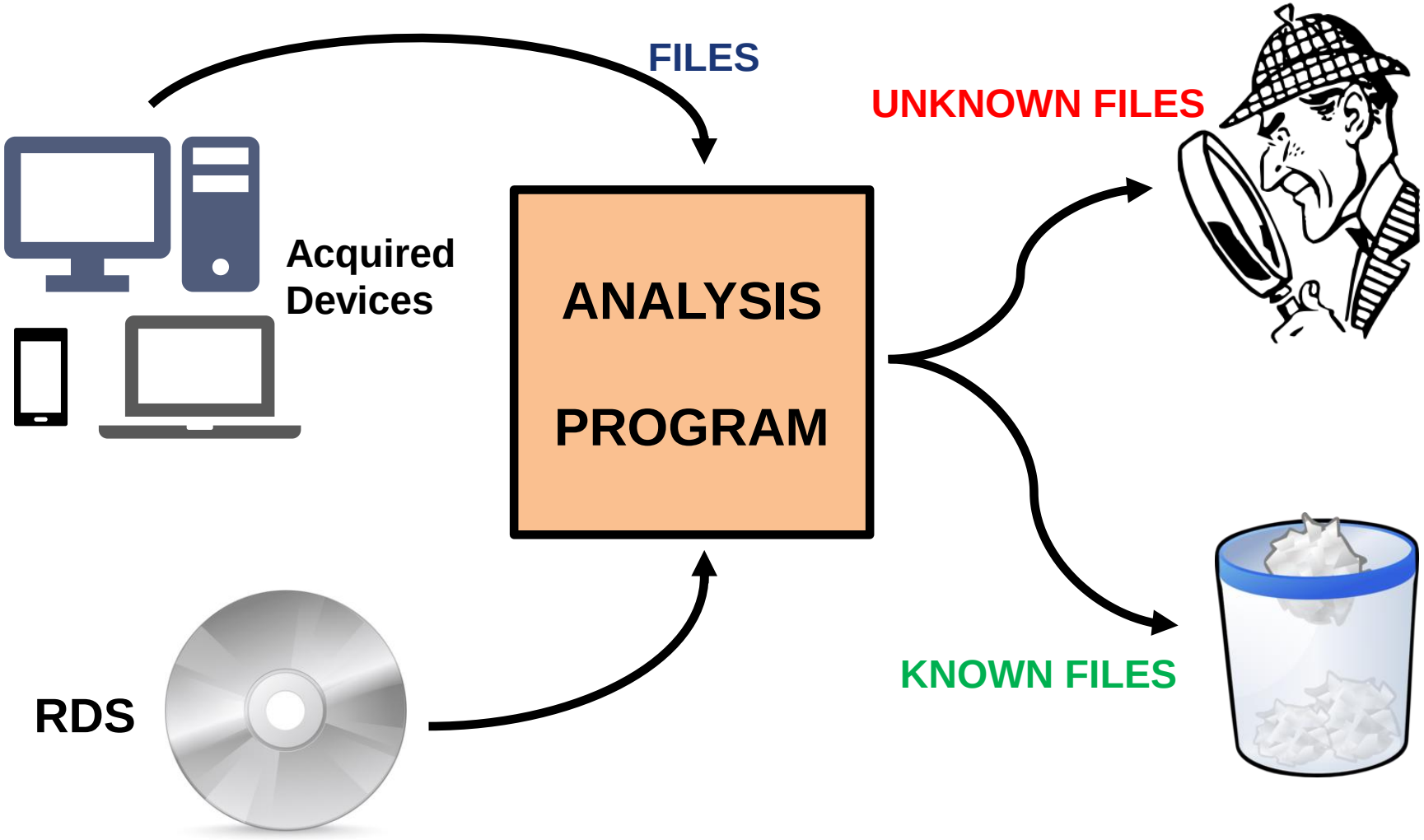
- The NSRL was established in 1999 to aid in the automated filtering of digital evidence
- The three objects of the NSRL
  - Collection of physical and digital software
  - Database of software meta-information
  - Published Reference Data Set (RDS)
- Goal: collect as much useful software as possible, and publish data helpful to investigations

NSRL Critical Data

- Software metadata
  - Application name, version, application type
  - Manufacturer info
  - OS info
  - Languages
- Cryptographic hashes
  - SHA256, SHA1, MD5

- Over 280 Million file hashes published across NSRL RDS sets

Uses of the NSRL RDS



Software Collection

- Types of software collected
  - Floppy disks, CDs, digital downloads, disk prints, mobile device applications, PC games, and more

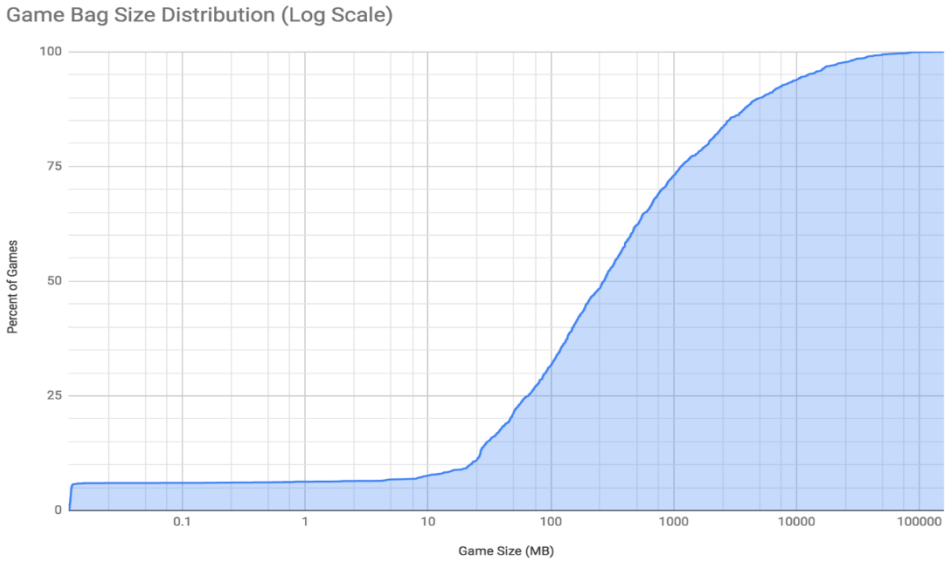
- Need popular software
- Need software that's common on an average computer
- Need software that may be used criminally

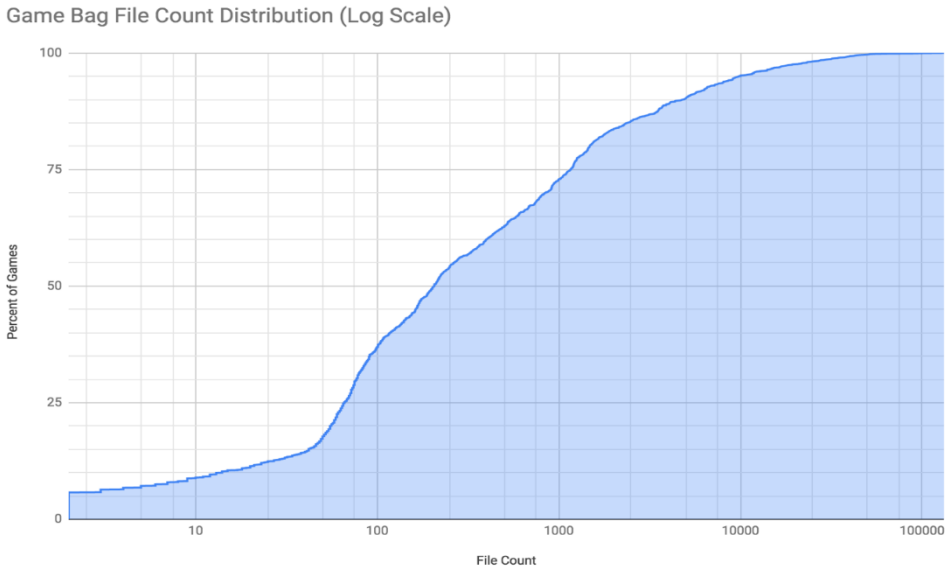
Why the NSRL Collects Games

- Computer games are very popular
- Thousands of games are free across multiple platforms
- Games may account for many files on an acquired device
- Games may have large amounts of multimedia files

Game Statistics

- 1,799 games collected
- 7,544 distinct versions of the 1,799 games
- Over half a million file hashes across all games collected
- 27% of games are larger than 1G
- 27% of games have more than 1,000 files

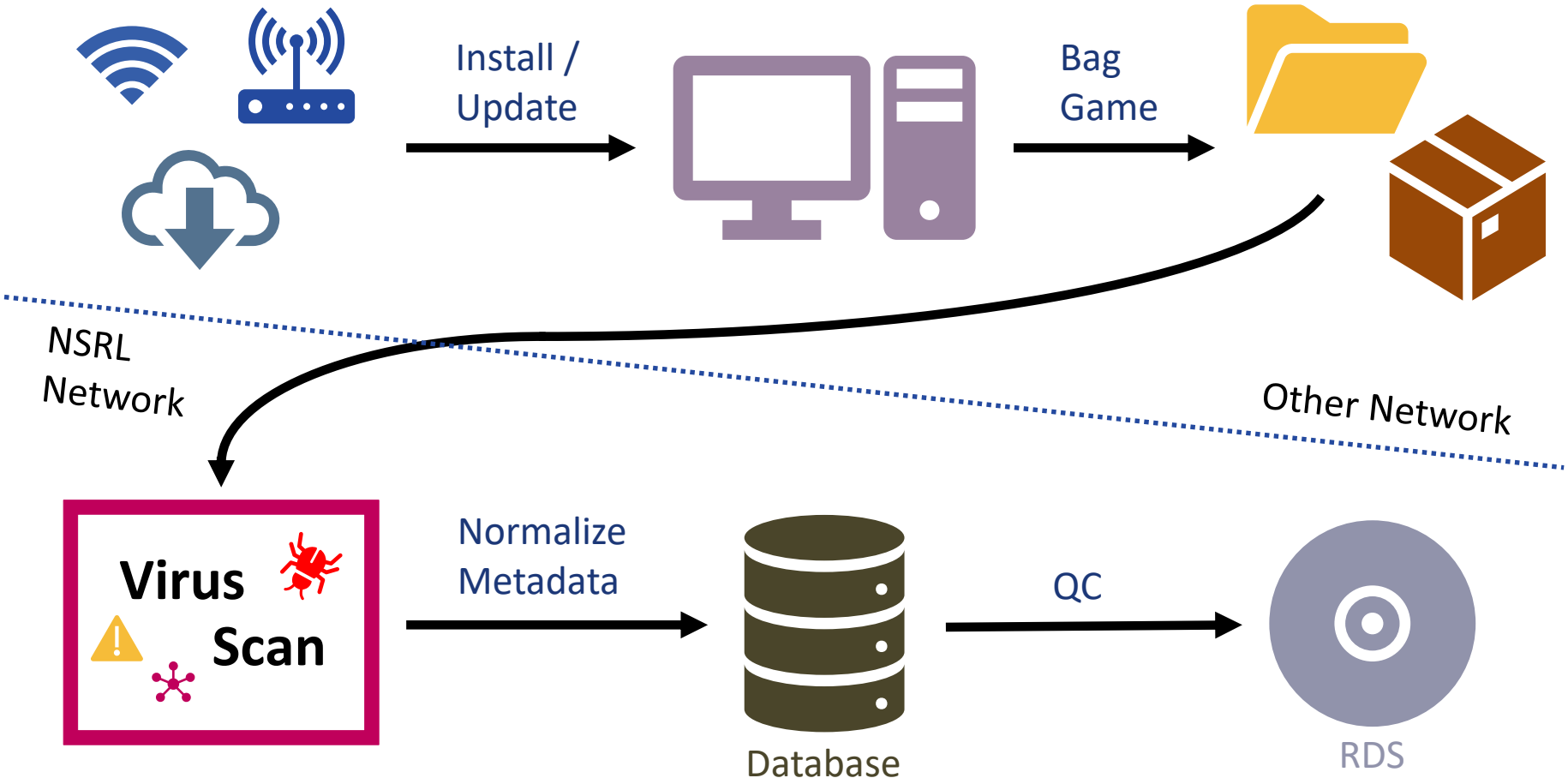




What Games do we Collect?

- We collect games from some of the largest gaming market places:
  - Blizzard (Activision Blizzard)
  - Origin (Electronic Arts)
  - Steam (Valve Software)
  - And soon, Epic Games
- We focus on games that are most popular now, and were popular in the past
  - We use publicly available popularity metrics to determine game popularity

Games Collection Process



Impacts of Game Collection

- Additions to the RDS
- Working on games has impacted development work in forensic formats, like AFF4
- Working on the games workflow has lead to internal NSRL improvements, and moved us closer to a new RDS format, which would include SHA256 hashes
- Working with games has spurred us to find better identifiers for the supply chain of software, in the form of SWID tags

We are always open to suggestions for new software to collect

Let us know at nsrl@nist.gov