Amcache Forensic Cheat Sheet

Field	Details
Location	C:\Windows\AppCompat\Programs\Amcache.hve
Purpose	Windows Application Compatibility artifact — logs program execution and installer metadata.

■ Key Data Stored

• Program path & name
• SHA1 hash of executable
• Compile time (PE header)
• File size
• First run time
• Created/Modified timestamps
• Version, description, publisher

■ Analyst Uses

• Confirm program execution (even if deleted)
• Build timelines of first run vs modification
• Link hash values to known malware
• Cross-check with Prefetch, Shimcache, SRUM, MFT
• Detect suspicious or deleted executables

■ Tips

• Look for mismatched compile vs run times → may indicate quick malware execution.
• If Prefetch disabled, Amcache may still show program activity.
• Entries remain even if program is uninstalled or deleted.
• Combine with $MFT timestamps for stronger attribution.