ForenClarity

ForenClarity for Windows v1.0.0 Commercial

Complete User/Admin Documentation, Installation Guide, Uninstall Guide, and QA Notes

Product	ForenClarity for Windows
Version	v1.0.0 Commercial
Customer-facing build label	Windows v1.0.0
Internal documentation baseline	Accepted lifecycle baseline Build17
Prepared for	Website/download documentation and saved release folder

Important: Customer-facing documentation uses the clean product version name. The internal Build17 reference is preserved only for traceability and QA records.

Table of Contents

1. Product purpose and scope

ForenClarity is an evidence clarity and triage assistant. It is designed to help administrators quickly read endpoint, network, Defender, startup, service, process, firewall, and optional local-engine evidence. It is not a replacement for antivirus, EDR, SIEM, firewall management, full forensic investigation, or incident-response tooling. The value is clarity: collect useful signals, reduce security fatigue, and present practical next steps in reports and dashboard views.

Plain-English positioning

Item	Meaning / action
Primary problem	Security teams and small administrators can be overwhelmed by logs, alerts, open ports, services, AV events, firewall events, and connection data.
ForenClarity role	Turn scattered evidence into a readable triage view and report, with clear next steps.
Customer promise	Evidence clarity and admin guidance; no fake claim that the system is compromise-free.
Commercial scope	Windows v1.0.0 and Ubuntu v1.0.4 are the first stable public targets. Parrot and Kali are planned/coming soon.

2. What ForenClarity does and does not do

Capabilities

Item	Meaning / action
Endpoint evidence	Collects and summarizes processes, services, startup items, scheduled tasks, Defender/AV status, PowerShell events, and Windows security signals where available.
Network evidence	Summarizes listening ports, established connections, external/remote connections, firewall log status, packet-capture readiness, and passive scan/probing evidence.
Reports	Exports readable full security reports and network monitor reports. CSV files remain the technical evidence record.
Advanced Sources	Shows admin-only details for optional local engines and future integrations. Main dashboard stays clean.
License/trial state	Uses a protected local cache for the current 60-day trial placeholder.

Non-goals and limitations

Item	Meaning / action
Not AV/EDR/SIEM	ForenClarity does not replace Microsoft Defender, EDR, SIEM, firewall management, forensic investigation, or incident response.
No proof of safety	A Clean result means no enabled ForenClarity rule produced a suspicious finding in that scan. It does not prove the system is compromise-free.
Optional engine limitations	Snort/Suricata are admin-controlled local engines. Future Zeek/SIEM/pfSense-style integrations remain planned until safely tested.
External dependencies	Python, Npcap, Wireshark, Snort, and Suricata may remain after uninstall and should be reviewed manually.

3. System requirements and dependencies

Supported environment

Item	Meaning / action
Operating system	Windows 10/11 x64 style environment. The accepted test VM was Windows 10 x64.
Privileges	Administrator rights are required for install, uninstall, firewall access repair, optional dependency installation, and local engine actions.
Network	Internet is useful for dependency acquisition and updates. Local evidence collection still works within the installed scope.
Security software	Microsoft Defender is supported as the native AV provider in this build.

External components

Item	Meaning / action
Python	Runtime used by the Windows application package. Do not remove manually if other software needs it.
Npcap	Packet capture driver used for capture readiness and future scan attribution workflows.
Wireshark	Optional but useful for packet capture validation and admin troubleshooting.
Snort	Optional local IDS engine, controlled by admin action. Not silently restarted by ForenClarity.
Suricata	Optional local IDS engine, controlled by admin action. Not silently restarted by ForenClarity.

4. Installation guide

Use the Windows installer from the official ForenClarity download package. Until code signing is added, Windows may show an Unknown Publisher/UAC warning. This is expected for the current commercial baseline and should be resolved later with code signing.

Installation steps

Item	Meaning / action
1. Prepare the machine	Use an administrator account. Close old ForenClarity windows before reinstalling.
2. Run the installer	Launch the ForenClarity Windows v1.0.0 setup executable. Approve UAC.
3. Follow prompts	Allow required components only when appropriate for the machine. Do not force dependency removal or reboot.
4. Start application	Use the desktop shortcut or Start Menu entry. Some startup behavior may launch automatically depending on settings.
5. First scan	Open the dashboard and press Scan Now, or wait for the scheduled interval.
6. Export reports	Use Export Security Report and Network Monitor as needed.

Main dashboard after a clean scan

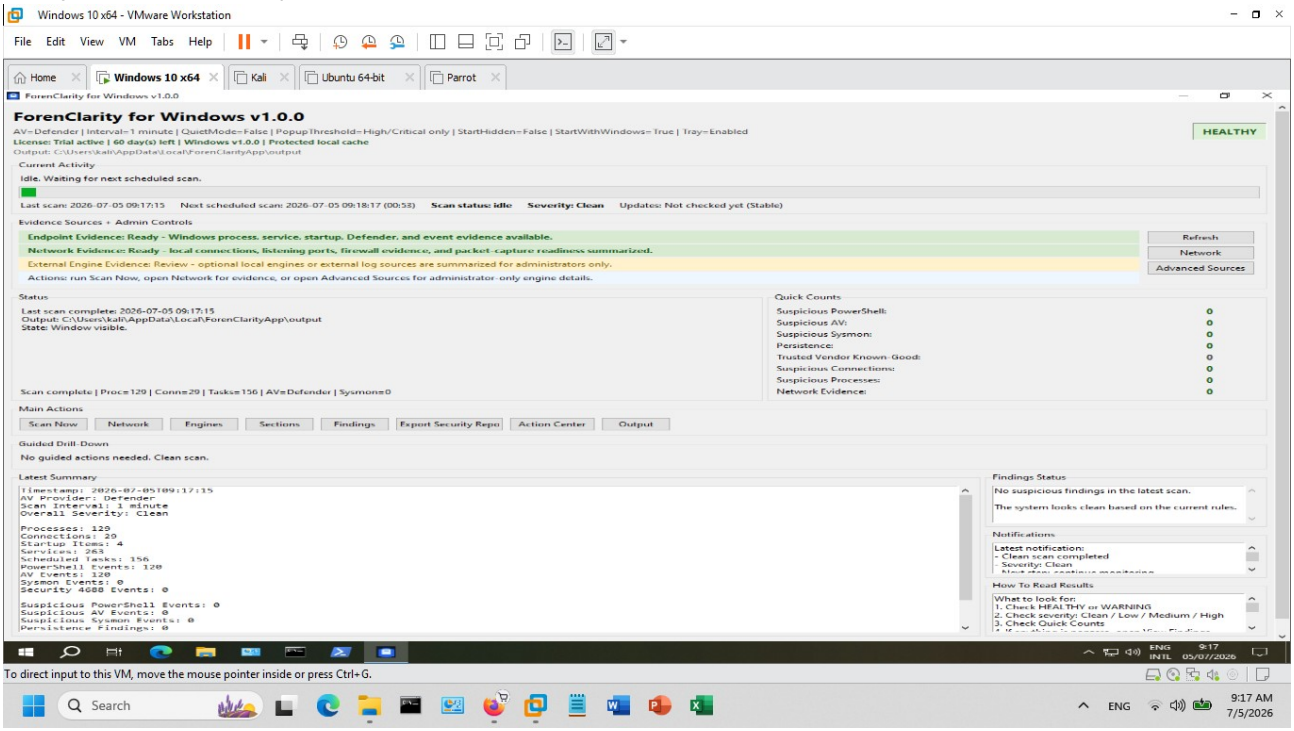

Figure: Main dashboard after a clean scan

5. Main dashboard explained line by line

Header and license lines

Item	Meaning / action
ForenClarity for Windows v1.0.0	Clean customer-facing product title.
AV=Defender	Native Defender evidence provider is detected and used.
Interval=1 minute	Scheduled scan interval in the current configuration.
QuietMode=False	Normal UI notifications/status are enabled.
PopupThreshold=High/Critical only	Popups are limited to high or critical conditions to reduce alert fatigue.
StartHidden=False	The application does not start hidden in the tested configuration.
StartWithWindows=True	Startup registration is enabled.
Tray=Enabled	Tray behavior is enabled when the app supports it.
License: Trial active | 60 day(s) left	Current protected local trial state.
Windows v1.0.0 | Protected local cache	Shows product version and local license/cache protection state.
Output path	Folder where reports, CSV files, summaries, and evidence outputs are written.

Current Activity and status

Item	Meaning / action
Idle / waiting for next scheduled scan	No scan is currently running.
Last scan	Timestamp of the latest completed scan.
Next scheduled scan	Next automatic scan time and countdown.
Scan status	Idle, in progress, or related processing state.
Severity	Highest ForenClarity severity from the latest enabled rule set.
Updates	Update status of the local stable package/rules where available.

HEALTHY	High-level health indicator based on current ForenClarity rules and readiness.

Evidence source rows

Item	Meaning / action
Endpoint Evidence: Ready	Windows process, service, startup, Defender, and event evidence are available.
Network Evidence: Ready	Local connections, listening ports, firewall evidence, and packet-capture readiness are summarized.
External Engine Evidence: Review	Optional local engines or external log sources are summarized for administrators only.
Actions	Recommended next actions, such as Scan Now, Network, or Advanced Sources.

Main action buttons

Item	Meaning / action
Scan Now	Runs an immediate evidence refresh.
Network	Opens the Network Monitor dashboard.
Engines	Opens local engine/admin source details where available.
Sections	Controls visible network monitor sections.
Findings	Opens findings overview from the latest findings CSV.
Export Security Report	Creates a readable full security report.
Action Center	Groups less-used actions so the main dashboard stays clean.
Output	Opens the output folder.

6. Network Monitor explained

Network Monitor dashboard

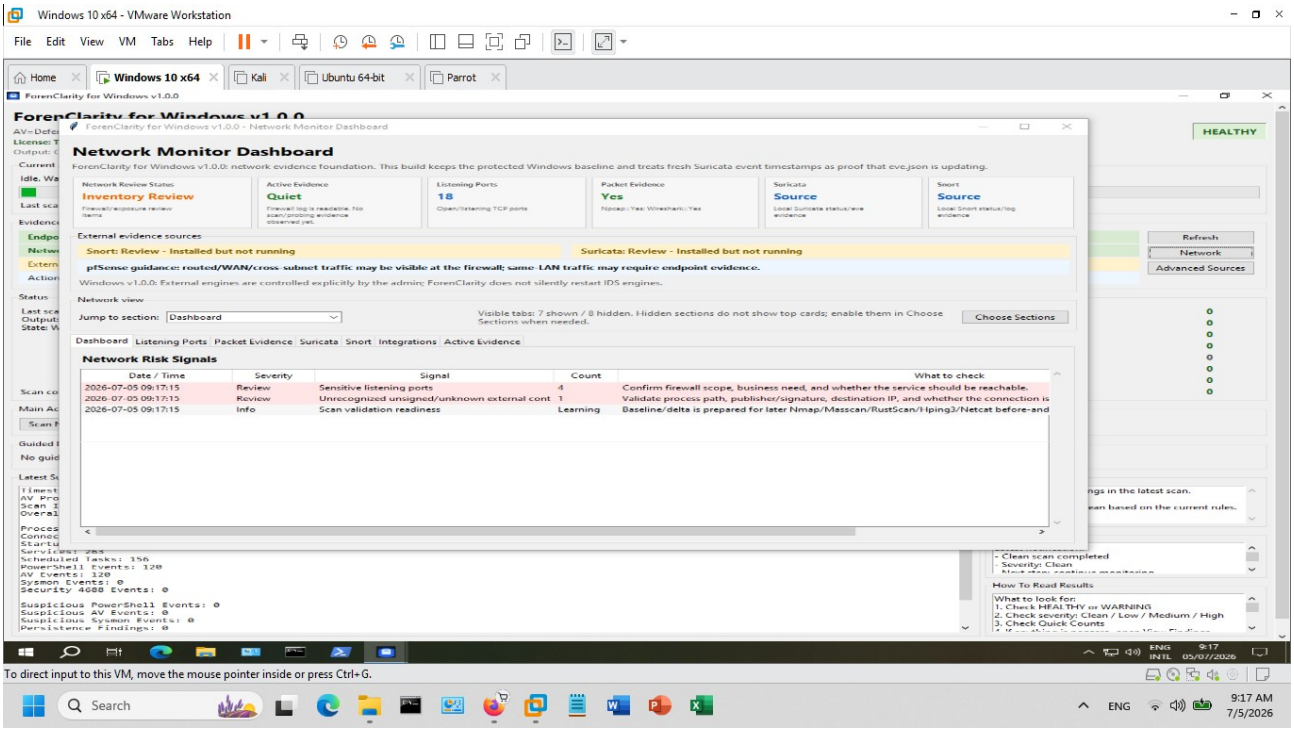

Figure: Network Monitor dashboard

Network top cards

Item	Meaning / action
Network Review Status	Inventory review, quiet, or alert state based on local network evidence.
Scan Evidence	Whether firewall/scan/probing evidence is currently observed.
Listening Ports	Count of open/listening TCP ports in the latest snapshot.
Packet Evidence	Npcap/Wireshark readiness and packet capture availability.
Suricata	Local Suricata status/evidence summary for administrator review.
Snort	Local Snort status/evidence summary for administrator review.

Network tabs

Item	Meaning / action
Dashboard	Plain-English risk signals and summary.
Listening Ports	Open ports and related process/service context.
Packet Evidence	Capture readiness and validation context.
Suricata	Suricata status, eve.json path, event types, and admin guidance.
Snort	Snort status, selected interface, config/log paths, and admin guidance.
Integrations	Planned or admin-only integration context.
Active Evidence	Current evidence view for the selected network snapshot.

7. Findings, reports, and output files

Findings overview

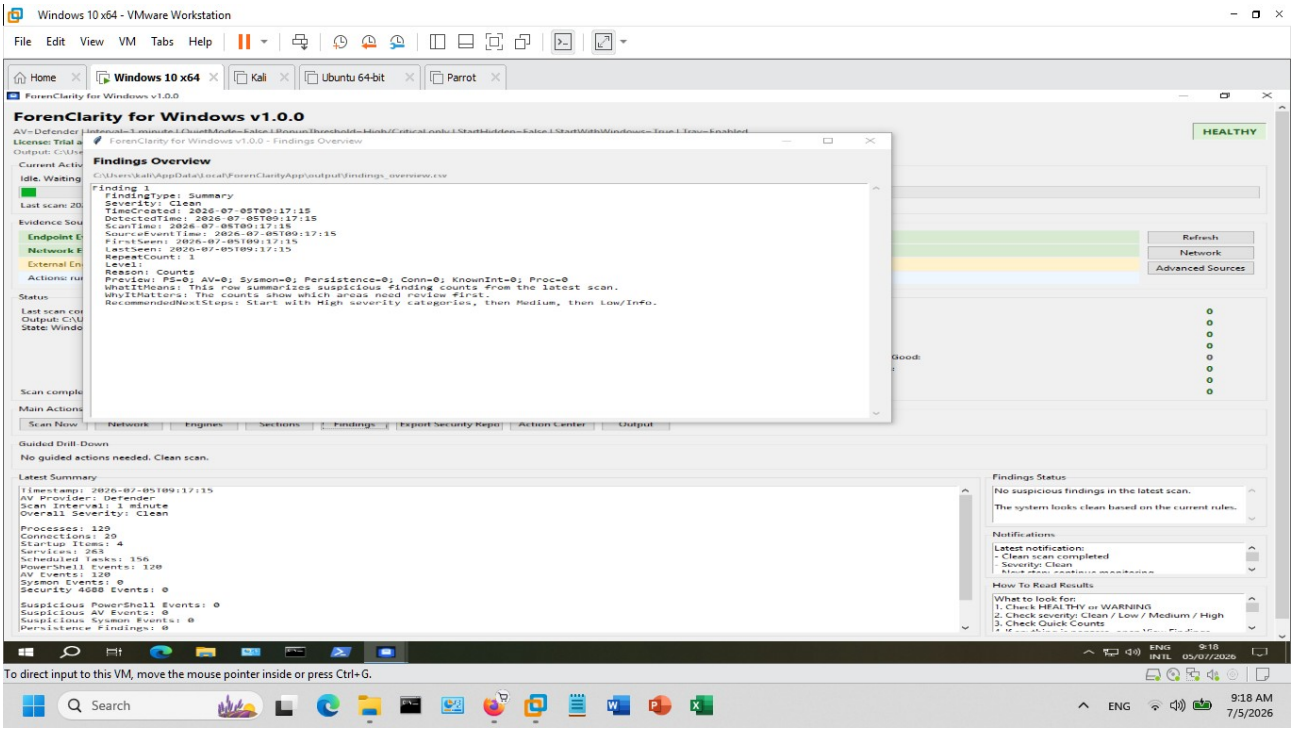

Figure: Findings overview

Findings fields

Item	Meaning / action
FindingId / FindingType	Unique finding identifier and category.
Severity	Clean, Info, Review, Low, Medium, High, or Critical depending on enabled rules.
Timestamp / DetectedTime / ScanTime	When the event was captured and processed.
SourceEventTime	Original event time when available.
RepeatCount	How many grouped occurrences were observed.
Reason	Why the finding appears.
WhatItMeans	Plain-English interpretation.
RecommendedNextSteps	Admin action guidance.

Important output locations

Item	Meaning / action
%LOCALAPPDATA%\ForenClarityApp\output	Primary report and CSV output folder.
full security report PDF/TXT	Readable admin/SOC handoff report.
network monitor report PDF/TXT	Readable network evidence report.
CSV files	Detailed technical evidence record for later review.
Desktop exported files	When the user exports or saves reports to the desktop.

8. Advanced Sources and optional engines

Advanced Sources / Engine Controls

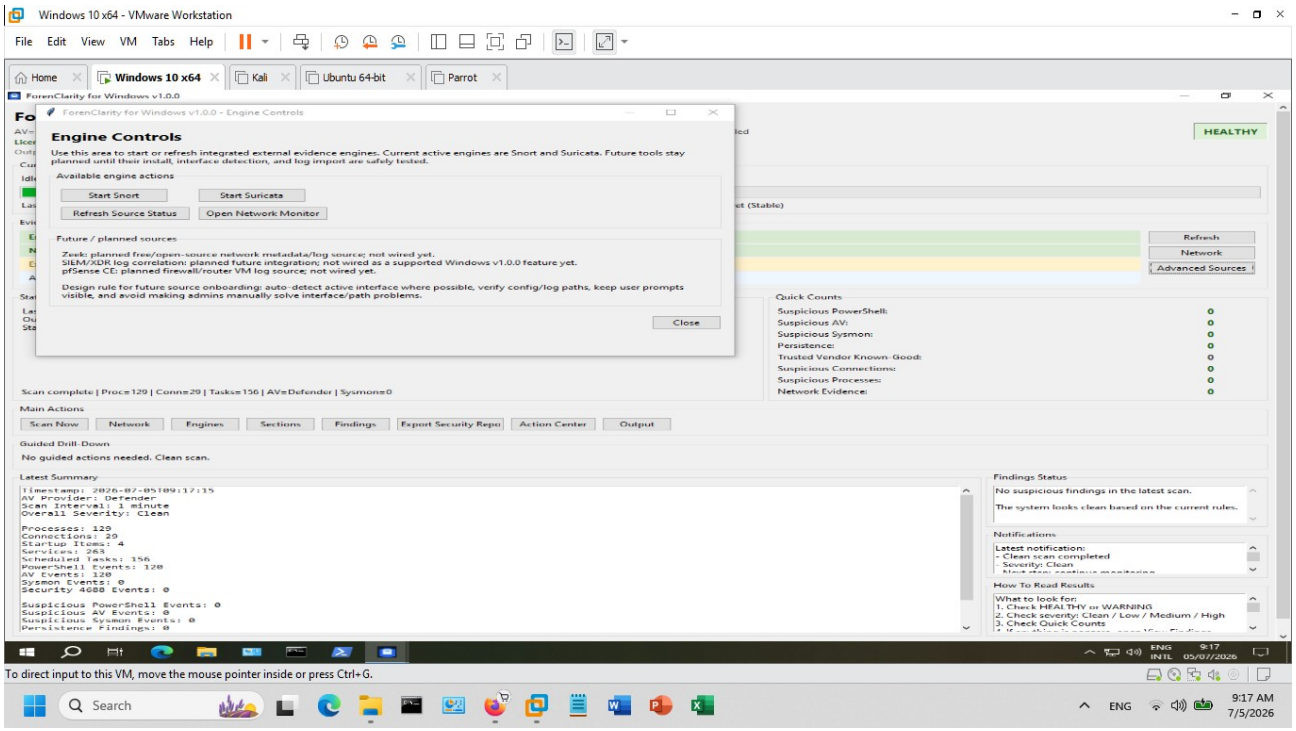

Figure: Advanced Sources / Engine Controls

Advanced controls

Item	Meaning / action
Start Snort	Admin action to start/use Snort where installed and configured.
Start Suricata	Admin action to start/use Suricata where installed and configured.

Refresh Sources	Refresh external/local engine status.
Open Network Monitor	Open network evidence dashboard.
Future planned sources	Zeek, SIEM/XDR log correlation, pfSense CE, and other sources remain planned until safely wired and tested.

9. Uninstall guide

ForenClarity Windows v1.0.0 Commercial removes the ForenClarity application, runtime process, shortcuts, startup entries, and optional ForenClarity data/license folders. External dependencies are not removed automatically by the accepted baseline; review them manually after uninstall.

Uninstall steps

Item	Meaning / action
1. Open Programs & Features	Control Panel > Programs > Programs and Features.
2. Select ForenClarity for Windows v1.0.0	Click Uninstall.
3. Approve UAC	Allow Windows to run the uninstall process.
4. Read dependency note	ForenClarity removes its own files only. External dependencies stay installed for manual review.
5. Choose report/settings cleanup	Choose Yes to remove ForenClarity reports/settings, or No to keep evidence.
6. Choose license-cache cleanup	Choose Yes to remove trial/license cache, or No to preserve licensing/trial state.
7. Read final result	The final panel must remain visible and state that dependencies require manual review.
8. Verify	Run the verification commands listed below.

Uninstall dependency notice

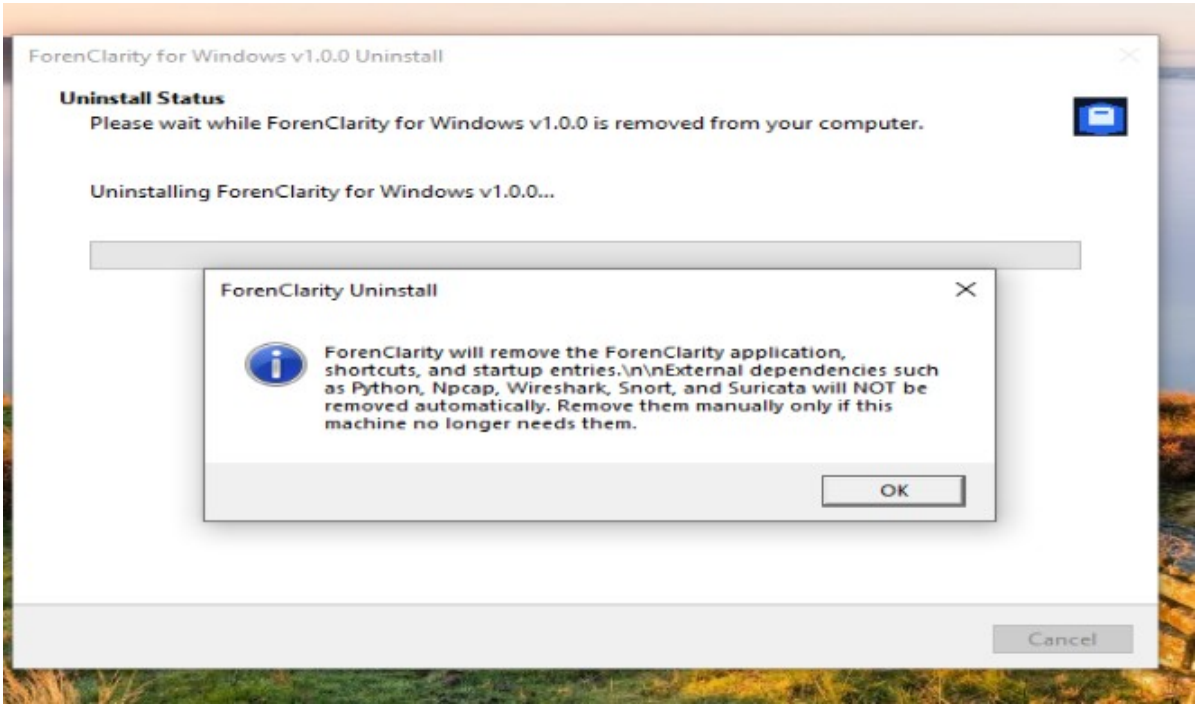

Figure: Uninstall dependency notice

Accepted Build17 uninstall result panel

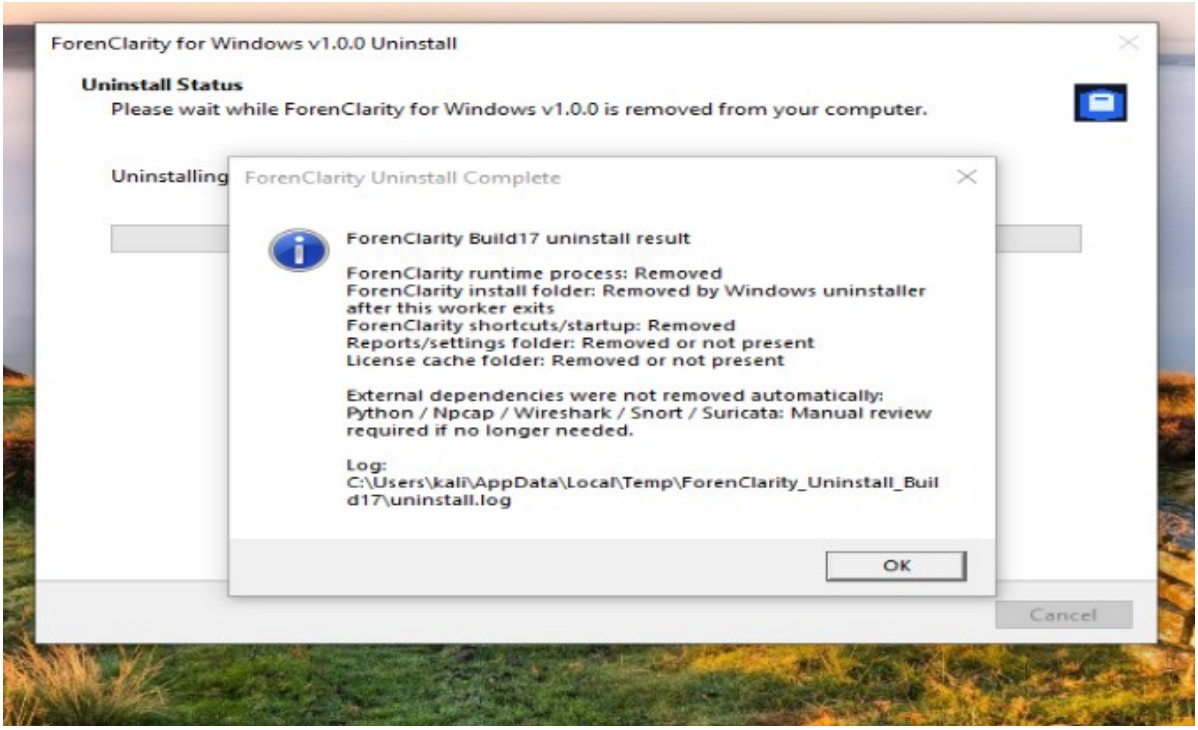

Figure: Accepted Build17 uninstall result panel

10. Manual dependency review

Do not blindly remove dependencies. Python, Npcap, Wireshark, Snort, and Suricata may be used by other security tools or workflows. Remove them manually only if the administrator confirms they are no longer needed.

Manual dependency guidance

Item	Meaning / action
Python	Remove from Windows Apps/Programs only if no other local tools depend on that Python installation.
Npcap	Remove only if no packet capture/network tools require it.
Wireshark	Remove only if packet inspection is no longer needed on the machine.
Snort	Remove only if the local IDS engine is not used independently.
Suricata	Remove only if the local IDS engine is not used independently.
Firewall logs folder	Do not forcibly remove C:\ForenClarityFirewallLogs if Windows Firewall logging still uses it.

11. Verification commands

After uninstall, verify that ForenClarity itself is gone. Dependency leftovers are expected unless the administrator removes them manually.

```
tasklist | findstr /i "python pythonw foren"
dir "C:\Users\%USERNAME%\AppData\Local\Programs\ForenClarity" /s /b
dir "%LOCALAPPDATA%" /b | findstr /i "Foren"
```

Expected verification result

Item	Meaning / action
Process check	No python/pythonw/ForenClarity process related to the app should remain.
Install folder check	File Not Found for %LOCALAPPDATA% \Programs\ForenClarity.
Data/license check	No ForenClarityApp/ForenClarityLicense if the admin chose to remove them. They may remain if preserved.

12. Troubleshooting

Common issues

Item	Meaning / action
Unknown Publisher	Expected until code signing is added. This is not the same as a product integrity failure.
Integrity manifest signature check failed	Do not use that package. It indicates package/protection mismatch.
Dependency still installed after uninstall	Expected in the accepted baseline. Review manually if no longer needed.
App still running after uninstall	Not acceptable. Verify tasklist and report the process command line.
Firewall log access issue	Run the Repair Firewall Log Access action as administrator.
No suspicious findings	Means no enabled rule fired. It does not prove the machine is compromise-free.

13. QA acceptance summary

Accepted Windows lifecycle baseline

Item	Meaning / action
Accepted product label	ForenClarity for Windows v1.0.0 Commercial
Internal baseline	Build17 accepted as Windows uninstall lifecycle baseline.
Accepted uninstall result	Runtime process removed, install folder removed by Windows uninstaller, shortcuts/startup removed, reports/settings and license cache removed or not present.
Final command result	tasklist check returned no python/pythonw/ForenClarity output; install-folder check returned File Not Found.
Dependency policy	External dependencies not removed automatically; manual review required.

14. Website/download page notes

Website copy requirements

Item	Meaning / action
Download platforms	Offer Windows and Ubuntu first.
Coming soon	Mark Parrot and Kali as Coming Soon.
Honest positioning	Evidence clarity, triage, readable reports, reduced alert fatigue; no fake marketing.
Uninstall note	Clearly state that Windows external dependencies may remain and require manual review.