ClueTracker

Monitorización en tiempo real de configuraciones en hosts remotos

Junio 2019

Javier Bravo Fernández

Grado en Ingeniería Informática
Administración de redes y sistemas operativos

Manuel Jesús Mendoza Flores
Fernándo Pérez López

Agenda

1. Introducción
2. Análisis
3. Diseño
4. Desarrollo y depuración
5. Demostración
6. Conclusiones
7. Ruegos y preguntas

1. Introducción

Contexto y justificación

Necesidades

Conocer de forma inmediata las configuraciones aplicadas en un PC de la red

Confirmar aplicación de parches
Versión de software instalado
Existencia de una dll
Versión de un fichero
Valor de una clave de registro
…

Opciones habituales

Scripts ad-hoc

Tiempo desarrollo - Diversidad scripts - Outputs no unificados

Herramientas Comerciales

Infraestructura – Servidores - Agentes
Configuraciones - Retardo en los informes

1. Introducción

Objetivos

Aplicación para escanear valores en hosts remotos conectados a la red

Principales

- **Paradigma Standalone**
- **Instalación sencilla**
- **Versatilidad**
- **Escalable**
- **Reducción de costes**

Parciales

- **Delimitación del entorno**
- **Selección de tecnología**
- **Configuración de seguridad**
- **Módulos**: Registro, sistema, Discos, Ficheros

1. Introducción

Metodología

Análisis

- Delimitación de entorno
- Selección de tecnología
- Seguridad

Diseño

- Módulo Principal
- Auxiliares
- Módulos específicos

Desarrollo

- Implementación
- Testeo
- Depuración

2. Análisis

Delimitación del entorno

Evaluación de los sistemas operativos más habituales, para orientar nuestra aplicación a un mayor mercado.

Market Share

Windows	**all**	**86,30%**
Mac OS	all	9,65%
Linux	all	2,14%
Others	all	1,91%
Non-Windows	**all**	**13,70%**

Fuente: Netmarkshare 2018-03 to 2019-02

Windows

es la plataforma más extendida en entornos empresariales.

2. Análisis

Selección de tecnología

Evaluación de tecnologías disponibles, y ponderación para su selección

Criterio		Puntuación				Puntuación ponderada			
	peso	vbscript	powershell	C#	C++	vbscript	powershell	C#	C++
Compatibilidad	5	5	3	5	5	25	15	25	25
Soporte a objetivos	4	3	3	5	5	12	12	20	20
Potencial en desarrollo	3	2	2	5	4	6	6	15	12
Bibliografía disponible	4	4	4	5	3	16	16	20	12
Experiencia previa	5	4	3	5	2	20	15	25	10
Coste	4	5	5	3	3	20	20	12	12
						99	**84**	**117**	**91**

C#

Es la tecnología que objetivamente más conviene para el desarrollo de la aplicación

2. Análisis

Seguridad

Análisis de las configuraciones previas necesarias para el correcto funcionamiento de una solución de este tipo

Función	Requisito
General	- Microsoft Windows x32 (all versions)
Acceso registro remoto	- Firewall Windows: permitir administración remota - Usuario y password configurados (no en blanco) - Servicio "Registro remoto" running
WMI	- Firewall Windows: permitir tráfico WMI - UAC: cuenta de dominio incluida en administradores locales de los equipos - DCOM y CIMOM: no requiere ajustes si trabajamos con cuentas de dominio

3. Diseño

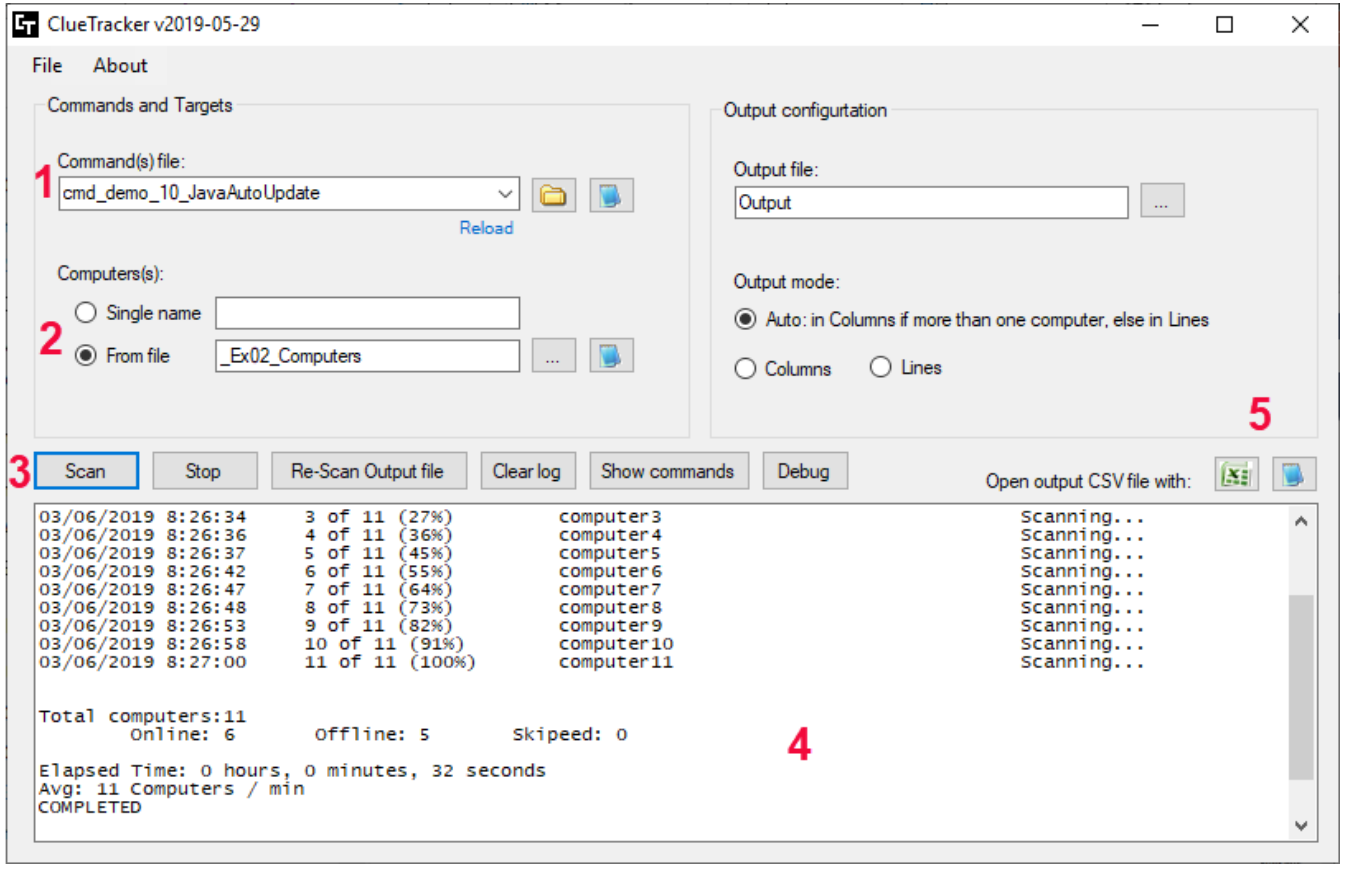
Arquitectura

La aplicación se estructura en capas: un Módulo Principal que hace de interfaz de usuario y los Módulos Específicos. Se añade una capa de Funciones Auxiliares

Principal	Main
Específicos	Windows Registry; System Information; Logical Disk Information; Files Information
Auxiliares	Procesador de instrucciones; Gestión de Ouptut; Gestión de excepciones

3. Diseño: Módulo Principal

Interfaz de usuario



Controles principales

1: Commands: administración y selección de los ficheros deconsultas

2: Computers: administración y selección de equipos sobre los que lanzar las consultas.

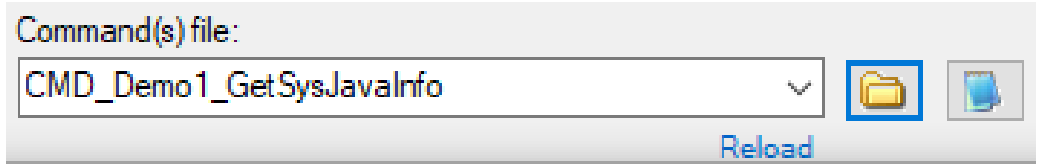
3: Controles principales

4: Log de progreso de los escaneos y actividad de la aplicación.

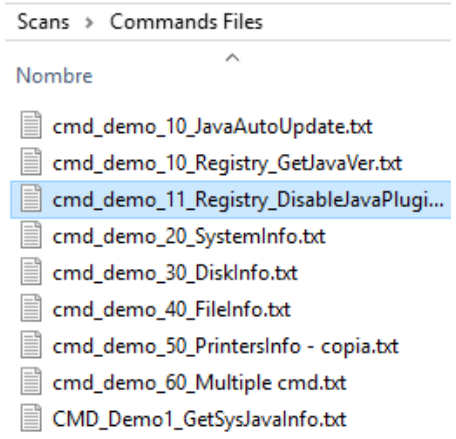
5: Outputs: Visualización y formateado.

3. Diseño: Módulo Principal

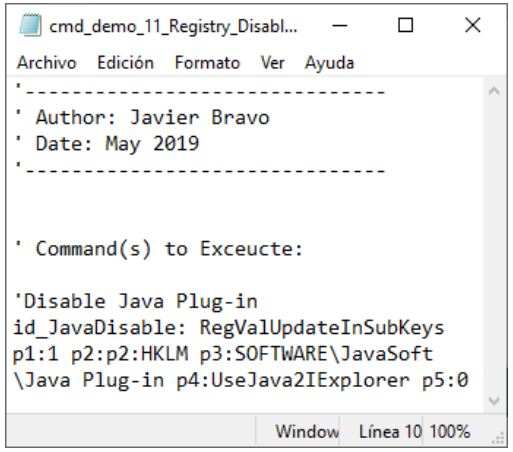
Ficheros de consultas



Consultas guardadas



Fichero de consulta



Comandos

El usuario puede **guardar consultas** personalizadas.

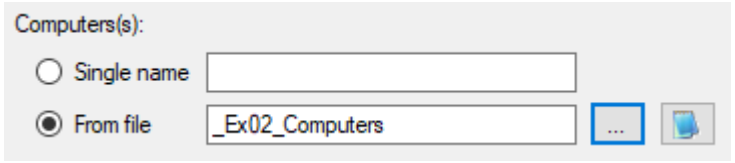
Es posible **combinar consultas** de diferentes módulos en un mismo fichero: Registro, Sistema, Discos, Ficheros

El fichero permite **introducir comentarios** para una mejor comprensión del propósito de cada fichero

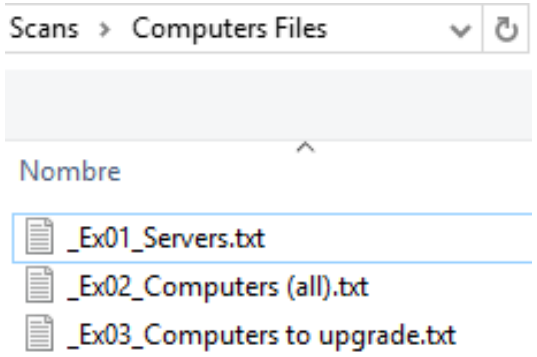
Acceso directo a la **carpeta de ficheros** con comandos, y a la **edición directa** del fichero seleccionado

3. Diseño: Módulo Principal

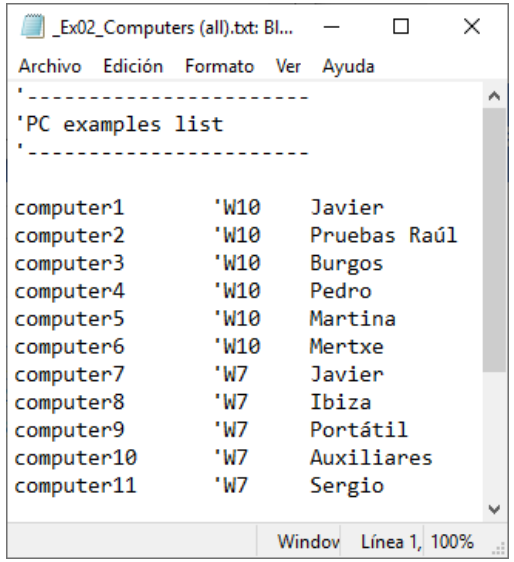
Fecheros de hosts



Listados de hosts



Fichero de hosts



Computers

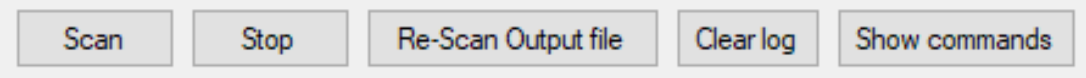
El usuario puede **guardar listados** diferentes de hosts, permitiendo tener listados **para cada propósito**

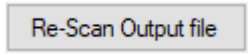
Para **escanear un host puntual**, es posible introducir el nombre de host directamente, sin tener que seleccionar ningún fichero.

El fichero permite **introducir comentarios** para una mejor comprensión del propósito del fichero, y detalles sobre cada uno de los hosts contenidos en el listado

3. Diseño: Módulo Principal

Controles principales



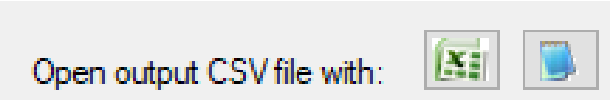


Re-Scan Otuput file: Relanza el escaneado tomando como listado de host el último ouptut generado, pero tratando de conectarse sólo a los hosts que anteriormente estaban offline y manteniendo para el resto el resultado leído en escaneos anteriores

Muestra los comandos disponibles junto a una descripción de los parámetros que requiere cada uno de ellos

3. Diseño: Módulo Principal

Output



	A	B	C	D	E	F	G
1	Computer Name	Date Time	Query	OuputVal_0	OuputVal_1	OuputVal_2	OuputVal_3
2	Computer Name	Date Time	id_SysInfo	ERROR: Invalid requested attribute name 'BIOSCaption			
3	Computer Name	Date Time	id_DiskInfo	Access	Availability	Caption	Compressed
4	Computer Name	Date Time	id_FileInf_winword2010.exe	Name	fileVersion	fileProductVersion	Length
5	Computer Name	Date Time	id_FileInf_winword2016.exe	Name	fileVersion	fileProductVersion	Length
6	Computer Name	Date Time	id_FileInf_excel2010.exe	Name	fileVersion	fileProductVersion	Length
7	Computer Name	Date Time	id_FileInf_excel2016.exe	Name	fileVersion	fileProductVersion	Length
8	Computer Name	Date Time	id_PrintersInfo	Caption	Default	DeviceID	Name
21	computer2	14/05/2019 17:18:23	id_FileInf_excel2016.exe	Not exists	Not exists	Not exists	Not exists
22	computer2	14/05/2019 17:18:23	id_PrintersInfo	ERROR: Access is denied. (Exception from HRE	N/A	N/A	N/A
23	computer3	14/05/2019 17:18:49	id_SysInfo	ERROR: The RPC server is unavailable. (Except	N/A	N/A	N/A
24	computer3	14/05/2019 17:18:49	id_DiskInfo	ERROR: The RPC server is unavailable. (Except	N/A	N/A	N/A
25	computer3	14/05/2019 17:18:49	id_FileInf_winword2010.exe	Not exists	Not exists	Not exists	Not exists
26	computer3	14/05/2019 17:18:49	id_FileInf_winword2016.exe	Not exists	Not exists	Not exists	Not exists
27	computer3	14/05/2019 17:18:49	id_FileInf_excel2010.exe	Not exists	Not exists	Not exists	Not exists
28	computer3	14/05/2019 17:18:49	id_FileInf_excel2016.exe	Not exists	Not exists	Not exists	Not exists
29	computer3	14/05/2019 17:18:49	id_PrintersInfo	ERROR: The RPC server is unavailable. (Except	N/A	N/A	N/A
30	computer4	14/05/2019 17:20:01	id_SysInfo	ERROR: Object reference not set to an instanc	N/A	N/A	N/A
31	computer4	14/05/2019 17:20:01	id_DiskInfo	0	No Info	C:	FALSE
32	computer4	14/05/2019 17:20:01	id_DiskInfo	0	No Info	D:	FALSE
33	computer4	14/05/2019 17:20:01	id_DiskInfo	No Info	No Info	E:	No Info
34	computer4	14/05/2019 17:20:01	id_FileInf_winword2010.exe	Not exists	Not exists	Not exists	Not exists
35	computer4	14/05/2019 17:20:01	id_FileInf_winword2016.exe	winword.exe	16.0.11425.20204	16.0.11425.20204	1971656
36	computer4	14/05/2019 17:20:01	id_FileInf_excel2010.exe	Not exists	Not exists	Not exists	Not exists
37	computer4	14/05/2019 17:20:01	id_FileInf_excel2016.exe	excel.exe	16.0.11425.20204	16.0.11425.20204	43708064
38	computer4	14/05/2019 17:20:01	id_PrintersInfo	Send To OneNote 2016	FALSE	Send To OneNote 2016	Send To OneNote 2016
39	computer4	14/05/2019 17:20:01	id_PrintersInfo	Microsoft XPS Document Writer	FALSE	Microsoft XPS Document Writer	Microsoft XPS Document Writer
40	computer4	14/05/2019 17:20:01	id_PrintersInfo	Microsoft Print to PDF	FALSE	Microsoft Print to PDF	Microsoft Print to PDF
41	computer4	14/05/2019 17:20:01	id_PrintersInfo	Fax	FALSE	Fax	Fax
42	computer5	14/05/2019 17:20:04	id_SysInfo	ERROR: Access is denied. (Exception from HRE	N/A	N/A	N/A
43	computer5	14/05/2019 17:20:04	id_DiskInfo	ERROR: Access is denied. (Exception from HRE	N/A	N/A	N/A
44	computer5	14/05/2019 17:20:04	id_FileInf_winword2010.exe	Not exists	Not exists	Not exists	Not exists
45	computer5	14/05/2019 17:20:04	id_FileInf_winword2016.exe	Not exists	Not exists	Not exists	Not exists

Output

El ouptut puede ser visualizado en modo **texto** o en **Excel**.

Al abrirlo en Excel, se **muestra formateado**. Si el fichero es multi-consulta, se mostrará una **cabecera** por cada consulta introducida.

Es posible **filtrar** por "Query" para simplificar los datos y **obtener una vista** correspondiente a **cada consulta** contenida en el ouptut

	A	B	C	D	E	F	G
1	Computer Name	Date Time	Query	OuputVal_0	OuputVal_1	OuputVal_2	OuputVal_3
3	Computer Name	Date Time	id_DiskInfo	Access	Availability	Caption	Compressed
24	computer3	14/05/2019 17:18:49	id_DiskInfo	ERROR: The RPC s	N/A	N/A	N/A
31	computer4	14/05/2019 17:20:01	id_DiskInfo	0	No Info	C:	FALSE
32	computer4	14/05/2019 17:20:01	id_DiskInfo	0	No Info	D:	FALSE
33	computer4	14/05/2019 17:20:01	id_DiskInfo	No Info	No Info	E:	No Info
43	computer5	14/05/2019 17:20:04	id_DiskInfo	ERROR: Access is d	N/A	N/A	N/A
50	computer6	14/05/2019 17:20:22	id_DiskInfo	ERROR: Access is d	N/A	N/A	N/A
57	computer7	14/05/2019 17:20:38	id_DiskInfo	ERROR: Access is d	N/A	N/A	N/A
64	computer8	14/05/2019 17:20:55	id_DiskInfo	_NO PING	_NO PING	_NO PING	_NO PING
71	computer9	14/05/2019 17:21:00	id_DiskInfo	ERROR: Access is d	N/A	N/A	N/A
78	computer10	14/05/2019 17:21:22	id_DiskInfo	0	No Info	C:	FALSE
79	computer10	14/05/2019 17:21:22	id_DiskInfo	0	No Info	D:	FALSE
89	computer11	14/05/2019 17:21:37	id_DiskInfo	0	No Info	C:	FALSE
90	computer11	14/05/2019 17:21:37	id_DiskInfo	0	No Info	D:	FALSE
91	computer11	14/05/2019 17:21:37	id_DiskInfo	No Info	No Info	E:	No Info

3. Diseño: Módulos específicos

Módulos específicos

Windows Registry	System Information	Files Information	Logical Disk	Printers
Búsqueda y modificación de claves hasta n subniveles a partir de una clave dada	Obtener parámetros del sistema (memoria, procesador, Sistema Operativo… etc.)	Obtener información y propiedades de un fichero indicando su path	Obtener información de las unidades de discos configuradas en el sistema	Obtener información de las impresoras configuradas en el sistema

3. Diseño: Módulos auxiliares

Módulos auxiliares

Procesador de instrucciones

Comprobación de **sintaxis** de las instrucciones.

Ayuda en pantalla al usuario en caso de errores de sintaxis

Gestión de Ouptut

Control de dimensiones (filas y columnas) para cada comando introducido.

Creación de cabeceras y filtros para **vistas simplificadas**

Gestión de excepciones

Control de excepciones en cualquiera de los módulos de la aplicación.

Información en pantalla de la excepción capturada y posibles recomendaciones.

4. Desarrollo y depuración

Preparación entorno de test

Hostname	Description	Location	Type	OS	Arch.
computer1	Javier Prod	LAN	Laptop	Windows 10 Pro	x64
computer2	Raúl Test	LAN	Laptop	Windows 10 Pro	x64
computer3	Wharehouse	WAN	Desktop	Windows 10 Pro	x64
computer4	IT PC	WAN	Desktop	Windows 10 Pro	x64
computer5	IT MM	LAN	Desktop	Windows 10 Pro	x64
computer6	IT MA	LAN	Desktop	Windows 10 Pro	x64
computer7	Javier Test	LAN	Desktop	Windows 7	X32
computer8	Distribution Center	WAN	Desktop	Windows 7	x86
computer9	Manager Laptop	WAN	Laptop	Windows 7	x86
computer10	Materials	WAN	Laptop	Windows 7	x86
computer11	IT EG	WAN	Laptop	Windows 7	x86
server1	FileServer1	LAN	Server	W2008	x64
server2	FileServer2	WAN	Server	W2003	x86
server3	AppServer1	WAN	Server	W2008 R2	x64
server4	AppServer2	WAN	Server	W2008 R2	x64
server5	AppServer3	WAN	Server	W2008 R2	x64
server6	AppServer4	WAN	Server	W2008 R2	x64

Se prepara un entorno con PC y servidores en diferentes versiones de Windows.

Aunque estaba fuera de los objetivos, se incluyen entornos x64 para verificar la compatibilidad

4. Desarrollo y depuración

Casos de test

Requerimiento	Test ID	Test a realizar	Pass / No Pass
Generales			
Standalone	1	Scan hosts remotos sin realizar configuraciones previas	OK
Instalación sencilla	2	La aplicación se inicializa correctamente sólo con abrir el ejecutable sin hacer configuraciones previas	OK
Minimización costes	3	Usabilidad completa sin necesidad de licencias	OK
Específicas			
Registro: Buscar Clave	4	Retorno del valor del registro consultado. Output muestra: - Offline: si está inaccesible - Error Permisos: si no tenemos privilegios	OK
Registro: Buscar subclaves	**5**	Retorno del valor del registro consultado.	OK
Registro: Actualizar valor	**6**	Sobreescribir valor. Output muestra: nuevo valor	OK
Registro: Actualizar valor en sublclave	**7**	Sobreescribir valor. Output muestra: nuevo valor	OK
Sistema	8	Retorno de todos los parámetros consultados.	OK
Unidades de disco	9	Retorno de todos los parámetros consultados.	OK
Ficheros	10	Retorno de todos los parámetros consultados O Fichero no encontrado.	OK
Impresoras	11	Retorno de todos los parámetros consultados.	OK
Usabilidad			
Guardado de consultas	12	Las consultas guardadas son seleccionables y reconfigrurables cada vez que abrimos la aplicación	OK
Inicialización del formulario	**13**	El formulario se abre con la última selección realizada por el usuario en cada uno de sus parámetros seleccionables	OK
Fichero multi-consulta	**14**	Retorno en un solo fichero de output de todos los valores definidos en el ejemplo.	OK
Output	15	Fichero Excel formateado, con cabeceras y filtros	OK
Errores de sintaxis en comandos	16	El log de la aplicación muestra el error detectado, indicando la línea conflictiva y no continúa con la ejecución	OK
Errores en ejecución	17	Los errores detectados al acceder a host remotos son capturados y reportados como mensaje en el ouput, para no interrumpir el escaneado del resto de hosts	OK
Errores de permisos	18	Se refleja en el ouptut para cada host	OK

Se ha establecido un juego de pruebas a realizar para validar el correcto funcionamiento de la aplicación y el cumplimiento de los objetivos.

Se recogen los resultados en una tabla donde comprobamos que todas las pruebas han sido correctas.

(*) Los **TestID en negrita** corresponden a funcionalidades adicionales que no estaban previstas en los objetivos iniciales del proyecto.

4. Desarrollo y depuración

Mejoras realizadas

Durante la fase de depuración se han detectado errores y se han aplicado algunas mejoras no previstas inicialmente

Windows x64

❗ No se ejecuta la app ni funcionan las consultas de registro remoto en hosts x64

✓ Se compila como Any CPU y se utilizan las clases .NET adecuadas para x64

Standalone

❗ Errores al mover ejecutable de un equipo a otro.

✓ Inicialización de variables no dependientes de instalación o configuración previa.

Usabilidad Output

❗ Output ilegible: nº diferente de columnas y filas en consultas múltiples

✓ Cabecera y filtro por comando introducido: se obtiene vista simplificada

5. Conclusiones

Autoevaluación

Puntos débiles

- **Complejidad técnica** subestimada
- **Gran dedicación** de tiempo al desarrollo técnico
- Impacto en tiempo disponible para elaboración de memoria y presentación

Puntos fuertes

- Los objetivos han sido alcanzados y en algunos casos superados (x64, impresoras… etc.)
- El diseño estructurado ha facilitado la escalabilidad y resolución de problemas
- Sin costes de licencias

5. Conclusiones

Líneas futuras

Ampliaciones técnicas

Copiado de ficheros desde un PC a otro(s), indicando los directorios

Recopilación de ficheros, por ejemplo, para recolectar logs de procesos locales en los PCs remotos.

Ejecución de scripts remotos, unido con los dos anteriores, nos permitiría copiar paquetes, ejecutarlos y recolectar los logs, para realizar tareas más avanzadas.

Oportunidades de venta

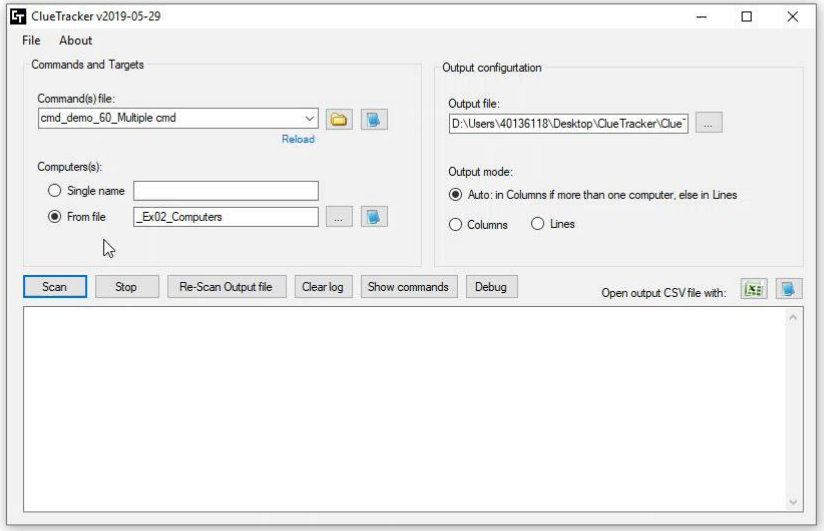
Segunda fase del proyecto, enfocada a la promoción, difusión y venta de la aplicación en PYMES.

Análisis de mercado, acceso a clientes

Análisis de **licenciamiento**, **distribución** y contratos de **mantenimiento**

6. Demostración

Demostración de uso de la aplicación en un entorno real



También disponible en YouTube

7. Ruegos y preguntas