



Comodo Forensic Analysis

Software Version 4.0

Administrator Guide

Guide Version 4.0.030119

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo Forensic Analysis	3
2 Run Forensic Analysis	4
2.1 The Main Interface	5
3 Scan Computers	6
3.1 Scan computers in an Active Directory domain	8
3.2 Scan Computers in a Workgroup	13
3.3 Scan Computers by Network Addresses	20
3.4 Scan your Local Computer	24
4 Scan Results	
5 Discover Computers	33
6 Reports	35
6.1 Executive Report	36
6.2 Device Report	37
6.3 Program Report	38
7 About Comodo Forensic Analysis	
8 Agent Requirements	41
About Comodo Security Solutions	42

COMODO Creating Trust Online

1 Introduction to Comodo Forensic Analysis

It is estimated that traditional antivirus software can only catch 40% of all malware in the world today. The other 60% are 'unknown'. An advanced persistent threat (APT) is an 'Unknown' piece of malware that is so well disguised it can be months before a traditional antivirus catches up to it. These malicious files reside on the victim's computer during this whole time, executing their payloads all the while.

Comodo Forensic Analysis (CFA) is a lightweight scanner which identifies unknown, and potentially malicious files, residing on your network. After scanning your systems, it will classify all audited files as 'Safe', 'Malicious' or 'Unknown'. While 'Safe' files are OK and 'Malicious' files should be deleted immediately, it is in the category of 'Unknown' that most zero-day threats are to be found. The CFA scanner automatically uploads these files to our Valkyrie servers where they will undergo a battery of run-time tests designed to reveal whether or not they are harmful. You can view a report of these tests in the CFA interface. You can also opt to have detailed scan reports sent to your email. The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis.

COMODO Forensic Analysis Tool			_ 🗆	×
Scan Completed (Files: 1384 Computers: 1 of 1)	Previous Scans	(IIII) Create Repo	ort 🍥 Options 🚺	Help
(1) 1382 (99.86%) Clean Files Clean Files Clean Files Clean Files Clean Files Clean Files			New Custom Scan Image: Detailed Scan Results Image: Detailed Scan Results <tr< td=""><td>à</td></tr<>	à
Name	er 2 Malizique 0	Size	Verdict	Y
 C\program files\windowsapps\microsoft.skypeapp_14.39.222.0 C\program files\windowsapps\microsoft.windows.photos_2019 C\program files\windowsapps\microsoft.skypeapp_14.39.222.0 	,x64_kzf8qxf38zg5c\skypebri. .18114.17710.0_x64_8wekyb ,x64_kzf8qxf38zg5c\skypepr	544 KB . 3 MB . 19 KB	No Threat Found Clean No Threat Found	
Please enter your email to receive a detailed scan results repo	nt: customermail@enterpri	se.com	Submit]
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solu	tions. Visit <u>one.comodo.com</u> t	to learn how Comodo	o can help protect your environ	ment.

Features

- No installation required, just run the portable application on any computer in the network
- Scan local machines or specify target endpoints by Active Directory, Work Group or network address. The scan discovers all computers available in a given network
- Unknown files are automatically uploaded to Comodo Valkyrie and tested for malicious behavior
- · Comprehensive reports provide granular details about the trust level of files on your endpoints

This guide takes you through the use of Comodo Forensic Analysis and is broken down into the following sections:

COMODO Creating Trust Online*

Comodo Forensic Analysis - Admin Guide

- Introduction to Comodo Forensic Analysis
- Run Forensic Analysis
- Scan Computers
 - Scan Computers in an AD Domain
 - Scan Computers in a Workgroup
 - Scan Computers by Network Addressees
 - Scan your Local Computer
- Scan Results
- Discover Computers
- Reports
 - Executive Report
 - Device Report
 - Program Report

2 Run Forensic Analysis

Comodo Forensic Analysis can be downloaded from https://enterprise.comodo.com/freeforensicanalysis/ After saving, you can launch the tool by double-clicking on the setup file. No installation is required.

COMODO Forensic Analysis Tool	b.	_ 🗆 ×
Discovery Completed	🕤 Previous Scans 🛯 👜 Create Report	Options (i) Help
34 Devices Found		E Scan Now Custom Scan
Q Search by Computers		
Name	IP	
10.108.51.10	10.108.51.10	
🔲 💂 Win10	10.108.51.12	
calltransfer044	10.108.51.36	
🔲 💭 seo014	10.108.51.53	
🔲 💭 SEC004	10.108.51.54	
🔲 💭 SEC001	10.108.51.56	
Seo003	10.108.51.58	
🔲 💭 SECOOS	10.108.51.60	
		44.07
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security soluti	ons. Visit <u>one.comodo.com</u> to learn how Comodo ca	n help protect your environment.

2.1 The Main Interface

The main interface of the tool allows you to configure and run scans, view results and generate risk reports.

COMODO Creating Trust Online

Title Bar Menu Bar	
COMODO Forensic Analysis Tool	_ 🗆 ×
Scan Completed (Files: 1405 Computers: 1 of 34) Scans (👜 Create Report 🍥 Options 🧃 Help
Image: Non-State State	Image: New Custom Scan Image: New Custom Scan Image: Detailed Scan Results Image: New Custom Scan Image: Start Discovery
Q Search by Computers	Group by
Name	Size Verdict 🖃
10.108.51.10 (10.108.51.10) Unknown error	Failed
Win10 (10.108.51.12) Login problem: invalid username or bad password.	Failed
Calltransfer044 (10.108.51.36) Unknown error	Failed
🔛 seo014 (10.108.51.53) Unknown error	Failed
SEO004 (10.108.51.54) Unknown error	Failed
SEO001 (10.108.51.56) Unknown error	Failed
Please enter your email to receive a detailed scan results report: customermail@enterprist Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit <u>one.comodo.com</u> to Email Form Area	e.com Submit

Main Functional Areas

- **Title Bar** Displays the scanning progress. You can also minimize, maximize and close the application by using the controls at the far right.
- Menu Bar Contains the controls for using the application.
 - Options Displays the port numbers that CFA uses to communicate with our file lookup service (FLS). The FLS is used to deliver real-time verdicts on the trust status of unknown files. Admins should leave these ports at the default.

Options				×
	FLS ICP Port	80		
1	FLS UDP Part	53		
				_
	Car	ncel	Save	

- Create Reports Generate a detailed report of the scan results. See 'Reports' for more details.
- Previous Scans Shows your most recent scans.
- Help The 'About' menu entry shows product and version information. Refer to 'About Comodo Forensic Analysis for more details. The 'Agent Requirements' menu entry contains troubleshooting advice if you experience problems connecting to your target computer.

COMODO Creating Trust Online*

- Search Allows administrators to search for listed endpoints by name.
- Main Display Area Displays details of scanned endpoints and the results from Valkyrie. Refer to the sections 'Scan Computers' and 'Scan Results' for more details. Also contains controls for launching local and custom scans:
 - Scan Now Scan endpoints on your local network to identify unknown files. Refer to section 'Scanning Computers' for more details.
 - New Custom Scan Scan endpoints in a Workgroup, Active Directory, or Network Addresses. You can also scan your local computer. Refer to the section 'Scan Computers' for more details.
 - Detailed Scan Results Opens Valkyrie results. Valkyrie is Comodo's file-verdict system, which
 comprehensively tests files to see if they exhibit malicious behaviour.
 - Start/Restart Discovery Identify the number of machines available in the given network. See Discover Computers for more details.
- Email Form Area Enter your email address after the Valkyrie analysis is complete to receive a detailed scan report.

3 Scan Computers

You can use any of the following methods to scan your target computers:

- Active Directory Suitable for a corporate environment where a large number of endpoints need to be scanned.
- Workgroup Scan computers that belong to a local work group
- Network Address Specify target endpoints by host name, IP address, or IP range
- This Computer Run a scan on your local device.

Unknown files discovered by the scan are automatically submitted to Comodo Valkyrie for further analysis. The Forensic Analysis tool shows results from the initial scan, and in-depth results from Valkyrie.



Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit <u>one.comodo.com</u> to learn how Comodo can help protect your environment.

COMODO Creating Trust Online*

- Previous Scans View the results of your recent scans in chronological order. Double-click on the name of the scan to view the last CFA scan result page
- Detailed Results View Valkyrie results. Files with an 'unknown' trust rating are uploaded to Valkyrie for more in-depth tests.
- Current Scan Return to the present results screen
- You can also use the search box to look for specific scan results:

COMODO Forensic Analysis Tool			_ 0
Previous Scans	Current Se	can 🐽 Create Repo	n 🍥 Options 🧃 F
Q Search			٩
Scan Summary	Scan Date	Scan Target	Scan Type
Computers scanned: 1. Total files scanned: 35260. Unknown: 7	2/25/2019 12:57:56 PM	Local Computer	Custom Scan Detailed Results
Scan Canceled.	2/26/2019 1:56:58 PM	Local Computer	Quick Scan
Scan Canceled.	2/26/2019 2:00:45 PM	Local Computer	Custom Scan
Computers scanned: 1. Total files scanned: 1344. Unknown: 0. M	2/26/2019 5:13:27 PM	Local Computer	Quick Scan Detailed Results
Sector and the sector of the sector of the sector of the sector of the	GEOREGES STOLET FM	computer	Detailed Ne

Refer to the following sections for more details:

- Scan computers in an Active Directory domain
- Scan computers in a Workgroup
- Scan computers by Network Address
- Scan your Local Computer

3.1 Scan computers in an Active Directory domain

The Active Directory method lets you import and scan all endpoints in a domain.

Click 'Custom Scan' on the home screen to open the scan wizard:

COMODO Creating Trust Online*

COMODO Forensic Analysis Too	1			-	$\square \times$
Discovery Completed		🕤 Previous Scans 🥡	Create Report	Options	(i) Help
34 Devices Found				Scan Now	ery
Q Search by Computers			ID		
 Name 10.108.51.10 			10.108.51.10		
🔲 💭 Win10			10.108.51.12		
			10 108 51 36		
Start Scan Wizard					×
Select Scan Targets					
Como	tive Directory n computers by cting them from ctive Directory		Network Scan cor specifying or endpo	Addresses nputers by IP addresses pint names	nent
+ : Scal Scal	Workgroup n computers by cting them from Workgroup		This Cor Scan this c	nputer omputer	
				Cancel	

- Select 'Active Directory' to open the AD configuration screen.
- Enter the domain name and login details of your Active Directory domain:

COMODO Creating Trust Online

Start Scan Wiza	ard			×
	Active Directory Creden	tials		
	Domain Name	Enter Domain Name		
	Domain Administrator	Enter Domain\Administrator		
	Password	Enter Password	Ø	
Back				Next

• After successful authentication, the 'Select Computers' screen will open. Choose the endpoints you want to scan then click next:

Start Scan Wizard	×
Select Computers	
⊿ 💌 test	
Computers	
Domain Controllers	
Back	Next

COMODO Creating Trust Online*

Start Scan Wiza	ard		×
	Scan Credentials		
	Login	Administrator	
	Password	•••••	~
Back		Quick Scan	Full Scan

- Next, choose one of the following scan types:
 - Quick Scan: Scans critical and commonly infected areas of target endpoints
 - Full Scan: Scans all files and folders on target endpoints.

COMODO Creating Trust Online*

37.20% Scan In Progress (Files: 6840] Computers: 0 of 7) Previous Scan Reports Options Stop Scan Stop Scan Stop Scan	COMODO Forensic Analysis Tool		-	- 🗆 ×
Image: September 2 (07.11%) Clean Files Image: September 2 (07.01%) Malicious Files Image: Septem	37.20% Scan In Progress (Files: 6840 Computers: 0 of 7) (Deprevious Scans (Marco R	eports	Options	(i) Help
Search By Computers Group By Image: Computers Name Size Verdict Image: Computers DESKTOP-TTPO9PR (10.108.51.100) 3120 scanned (4.57%). Unknown: 0. Malicious: 2. In Analysis 21. Im Progress TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password. Failed Image: VIIN-CU20X8JDY3D (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175. Im Progress Image: DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible. Offline Image: TOM (10.108.51.175) This computer is not accessible. Offline Image: TOM (10.108.51.175) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline	Image: Clean Files Image: Clean Files Image: Clean Files		● Stop	p Scan
Name Size Verdict Image: DESKTOP-TTP09PR (10.108.51.100) 3120 scanned (4.57%). Unknown: 0. Malicious: 2. In Analysis 21. Im Progress Image: TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password. Failed Image: WIN-CU20X8JDY3D (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175. Im Progress Image: DESKTOP-1AMD5C1 (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175. Im Progress Image: DESKTOP-1AMD5C1 (10.108.51.129) This computer is not accessible. Offline Image: SKYHIGH-PC (10.108.51.192) This computer is not accessible. Offline Image: TOM (10.108.51.175) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	Q Search By Computers		Group By	
Image: DESKTOP-TTPO9PR (10.108.51.100) 3120 scanned (4.57%). Unknown: 0. Malicious: 2. In Analysis 21. In Progress Image: TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password. Failed Image: WIN-CU20X8JDY3D (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175. In Progress Image: DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible. Offline Image: SKYHIGH-PC (10.108.51.192) This computer is not accessible. Offline Image: TOM (10.108.51.175) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Image: Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	Name	Size	Verdict	
Image: Convertige a detailed scan results report: customermail@enterprise.com Failed Image: Convertige a detailed scan results report: customermail@enterprise.com Failed Image: Convertige a detailed scan results report: customermail@enterprise.com Failed	DESKTOP-TTPO9PR (10.108.51.100) 3120 scanned (4.57%). Unknown: 0. Malicious: 2. In Analysis 21.		In Progress	
WIN-CU2OX8JDY3D (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175. In Progress DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible. Offline SKYHIGH-PC (10.108.51.192) This computer is not accessible. Offline TOM (10.108.51.175) This computer is not accessible. Offline WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password.		Failed	
DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible. offline SKYHIGH-PC (10.108.51.192) This computer is not accessible. Offline TOM (10.108.51.175) This computer is not accessible. offline WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	WIN-CU2OX8JDY3D (10.108.51.129) 3721 scanned (7.04%). Unknown: 0. Malicious: 0. In Analysis 175.		In Progress	
SKYHIGH-PC (10.108.51.192) This computer is not accessible. Offline TOM (10.108.51.175) This computer is not accessible. Offline WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible.		Offline	
Image: TOM (10.108.51.175) This computer is not accessible. Offline Image: WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	SKYHIGH-PC (10.108.51.192) This computer is not accessible.		Offline	
WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible. Offline Please enter your email to receive a detailed scan results report: customermail@enterprise.com	TOM (10.108.51.175) This computer is not accessible.		Offline	
Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit	WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible.		Offline	
Please enter your email to receive a detailed scan results report: customermail@enterprise.com Submit			_	
	Please enter your email to receive a detailed scan results report: customermail@enterprise.com		Subm	it

Scan progress is shown for each computer. Overall progress is shown on the title bar.

- Stop Scan Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:

COMODO Creating Trust Online*

ОМОДО For	rensic Analysis Toc	1				-	
can Completed (Fi	iles: 58864 Computers	: 2 of 7)	🕤 Previo	us Scans 🛛 👜	Create Report	t 🍥 Options	(î) н
58703 (99.73%) Clean Files	(0.01%) Malicious Files	94 (0.16%) Unknown Files	11 (0.02%) Failed	D 51 (0.09%) In Analysis		 New Custo Detailed Sc Start Discor 	m Scan an Results very
Q Search By Computer	75				Size	Group By	Q
DESKTOP-TTP	O9PR (10.108.51.100) C	ompleted: Total scanned: 3	33350. Unknown: 1	0. Malicious: 4. In A	512e	Completed	
CONYSTARK-F	PC (10.108.51.245) Login	problem: invalid usernam	e or bad password	L		Failed	
+ 🦉 WIN-CU2OX8	JDY3D (10.108.51.129)	ompleted: Total scanned:	25521. Unknown:	84. Malicious: 1. In J	A	Completed	
DESKTOP-1AM	4D5C1 (10.108.51.104) 1	his computer is not acces	sible.			Offline	
SKYHIGH-PC ((10.108.51.192) This com	puter is not accessible.				Offline	
TOM (10.108.5	51.175) This computer is i	not accessible.				Offline	
WIN-8719G19	COH7 (10.108.51.117) T	his computer is not access	ible.			Offline	
Please er	nter your email to receive a	a detailed scan results rep	ort: customerm	ail@enterprise.cor	π	Subr	nît

- There are two ways you can view the results:
 - **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
 - **Group by File**: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- **Detailed Scan Results** Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
 - Enter your email address in the field at the bottom
 - Click 'Submit' to receive the report at the address you supplied.

COMODO Creating Trust Online*

	E L	P DESKTOP-TTPO9PR (10.108.51.100) Completed: Total scanned: 85550 Urbritown: No. Mangoury 4 1974	····
	Ģ	P TONYSTARK-PC (10.108.51.245) Login problem: invalid username or bad password.	
	<u>ا</u>	P WIN-CU2OX8JDY3D (10.108.51.129) Completed: Total scanned: 25521. Unknown: 84. Malicious: 1. In A	
dias		DESKTOP-1AMD5C1 (10.108.51.104) This computer is not accessible.	Offline
		SKYHIGH-PC (10.108.51.192) This computer is not accessible.	Offline
		TOM (10.108.51.175) This computer is not accessible.	Offline
		WIN-8719G19C0H7 (10.108.51.117) This computer is not accessible.	Offline
		Please enter your email to receive a detailed scan results report: customermail@enterprise.com	Submit
Co	modo Fo	rensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Como	odo con help protect your environment.
	22222		
		When all the files are analyzed, you will receive a detailed report at comodo1@yopmail.com	Edit Email
363) 		Gol	o Settings to activate Windows.
Col	modo Fo	rensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Como	odo can help protect your environment.

Valkyrie results in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

VALKYRIE					SIGN IN 🗲
Forensic Analysis T	ool Scan Results				
FORENSIC ANALYSIS SCAN SESSION DETAILS Show 25					
File Name 🕴	Path \Rightarrow	SHA1	Last Activity 💡	Final Verdict 🕴	Human Ex
yoga.dll	c:\program files\windo	16a7e57546a6f1c83a5	2019-02-22 15:07:19	In Queue	Not Ready
skypeproxiesandstubs.dll	c:\program files\windo	cbd20af3001d36b95d5	2019-02-22 15:07:18	In Queue	Not Ready
chakrabridge.dll	c:\program files\windo	1af202ca17cc81c6029	2019-02-22 15:07:17	In Queue	Not Ready
skypeapp.dll	c:\program files\windo	45f9e25557117928669	2019-02-22 15:07:17	In Queue	Not Ready

Refer to the section 'Scan Results' for more details.

3.2 Scan Computers in a Workgroup

• Click 'Custom Scan' on the home screen to open the scan wizard:

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool				_ 0	×
Discovery Completed		Previous Scans (Create Report	Options ()	Help
34 Devices Found				E Scan Now Custom Scan	>
Q Search by Computers			ID.		
 Name 10.108.51.10 			1P 10.108.51.10		
🔲 🧕 Win10			10.108.51.12		
			10 108 51 96		7
🛛 Start Scan Wizard				X	
E Select Scan Targets					
Como + Acti Scan select Act	ive Directory a computers by ting them from tive Directory		Network Scan cor specifying or endp	Addresses mputers by IP addresses pint names	nent
+ : ··· For the second	Vorkgroup computers by ting them from Workgroup	Ø	This Cor Scan this o	mputer computer	
				Cancel	

- Click 'Workgroup'
- Select from available Workgroups, or enter the name of a Workgroup

COMODO Creating Trust Online*

Start Scan Wizar	d		×
	Specify Workgroup		
	Search Available Workgroups (m	ay take some time)	
	O Use Known Workgroup Name	Enter Workgroup Name	
Back			Next

• Select the computers you want to scan.

Start Scan Wiz	ard	×
	Select Computers	
	 COMODO TEST WELCOME WORKGROUP 	
Back		Next

COMODO Creating Trust Online*

- Next, enter the system's unique administrator username/password and choose one of the following scan types:
 - Quick Scan: Scans critical and commonly infected areas of target endpoints
 - Full Scan: Scans all files and folders on target endpoints.

Start Scan Wiza	ard			×
xxx 1	Scan Credentials			
	Login	Enter Login		
	Password	Enter Password	<i>•</i>	
Back		Quick Scan	Full Sca	an

After successful authentication, the scanning of endpoints in the Workgroup will start.

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool			-	. 🗆 :	×
38% Scan In Progress (Files: 1080 Computers: 0 of 1)	Previous Scans	(d) Create Report	Options	(i) He	lp
IO78 (99,81%) 2 (0.19%) Clean Files In Analysis			Stop Scan		
Q Search by Computers			Group by	Q G	
Name		Size	Verdict		
Iocalhost (127.0.0.1) 1080 files scanned (38.33%). Unknown: 0. Ma Iocalhost (127.0.0.1)	licious: 0. In Analysis 2.		In Progress		
Please enter your email to receive a detailed scan results repo	rt: customermail@enterp	rise.com	Subm	it	
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security sol	utions. Visit one.comodo.com	to learn how Comodo c	an help protect you	ar environm	ent

Scan progress is shown for each computer. Overall progress is shown on the title bar.

- Stop Scan Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:

OMODO Forensic Analysis Tool		_ 🗆 ×
Scan Completed (Files: 1405 Computers: 1 of 34)	🕤 Previous Scans 🏾 🐽 Cre	eate Report 🍥 Options (j) Help
Image: 1400 (99.64%) 5 (0.36%) Clean Files Unknown Files		Detailed Scan Results
Caution! Unknown/Potentially Malicious Files Comodo Forensic Analysis has scanned your environment and d sent to Comodo Valkyrie for analysis because any new malware email you a link to the results of Forensic Analysis in the next fer Comodo Advanced Endpoint Protection keeps your endpoints and reporting capabilities. It follows 'Default Deny' posture wh unknown files inside a secure container until a definitive verdict use such unknown files with no impact to the usability and yet	Are Found! detected unknown and thus potentially mal begins as an unknown file. Comodo Valkyr w hours. free from malware now and in the future an ich allows known files to freely run, blocks to of "good" or "bad" is delivered. Comodo A no harm to the system.	licious files which were iie file analysis platform will nd provides essential management bad files and automatically launches Auto-Containment™ feature allows to
SEO001 (10.108.51.56) Unknown error		Failed
P Sec003 (10.108.51.58) Unknown error		Failed
Please enter your email to receive a detailed scan results re	port: customermail@enterprise.com	Activate Windows
nodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security s	olutions. Visit one.comodo.com to learn ho	Go to Settings to activate Windows, w Comodo can help protect your environment

- COMODO Forensic Analysis Tool $\Box \times$ Scan Completed (Files: 1384 | Computers: 1 of 1) Previous Scans (m) Create Report (o) Options () Help New Custom Scan \mathbb{O} 1382 (99.86%) Q Search by Computers Name Size Verdict Iocalhost (127.0.0.1) Completed: Total files scanned: 1384. Unknown: 2. Malicious: 0. C\program files\windowsapps\microsoft.skypeapp_14.39.222.0_x64_kzf8qxf38zg5c\skypebri... No Threat Found 544 KB C\program files\windowsapps\microsoft.windows.photos_2019.18114.17710.0_x64__8wekyb... 3 MB Clean 🔥 c\program files\windowsapps\microsoft.skypeapp_14.39.222.0_x64_kzf8qxf38zg5c\skypepr... 19 KB No Threat Found Submit Please enter your email to receive a detailed scan results report: odo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can l
- The results interface contains details of each scan you have run along with verdicts for each file discovered

There are two ways you can view the results:

.

- **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
- **Group by** File: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- **Detailed Scan Results** Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
 - Enter your email address in the field at the bottom
 - Click 'Submit' to receive the report at the address you supplied.

COMODO Creating Trust Online*

VALKYRIE				I	SIGN IN
Forensic Analysis Tool S	can Results				
FORENSIC ANALYSIS SCAN S Show 25 v entries	Path	SHA1 $\stackrel{ {}_\circ}{=}$	Search: Last Activity 🚽	Final Verdict 崇	Hur
9CEBCF06E53458AD826B6336	\\127.0.0.1\C:\Window	713f318f4405fbc1b30a	2019-02-25 18:14:06	Clean	Clea
					Cicc
D5DD57BEAAE521AFDC067C6	\\127.0.0.1\C:\Window	cffb01b357a8b602aba	2019-02-25 18:14:05	Clean	Clea
D5DD57BEAAE521AFDC067C6 ED58CE97E4A9395A0C2075C9	\\127.0.0.1\C:\Window C:\Windows.old\Users\	cffb01b357a8b602aba 28f0d8c8650d6ed149e	2019-02-25 18:14:05 2019-02-25 18:14:04	Clean Clean	Clea

Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section 'Scan Results' for more details.

3.3 Scan Computers by Network Addresses

Scan computers by IP address/range, or host-name.

Click 'Custom Scan' on the home screen to open the scan wizard:

COMODO Creating Trust Online*

COMODO Forensic A	analysis Tool		_ 🗆 ×
Discovery Completed		Previous Scans Image: Previous Scans) Create Report 🛞 Options () Help
34 Devices Found			E Scan Now Custom Scan
Q Search by Computers			ID.
 Walle 10.108.51.10 			10.108.51.10
🔲 💭 Win10			10.108.51.12
Start Scan Wizar	d		10 108 51 36
្ Select Scan Targets ្			
Como	Active Directory Scan computers by selecting them from Active Directory		Network Addresses Scan computers by specifying IP addresses or endpoint names
+ :	Workgroup Scan computers by selecting them from Workgroup		This Computer Scan this computer
			Cancel

Select 'Network Addresses' to configure scan targets:

COMODO Creating Trust Online*

Start Scan Wizar	d		×
	Network Addresses		
		a	Add
	10.108.51.100/255.255.255.0		Remove
			Remove All
Back			Next

- Network Address: Enter the IP address, IP range or host name as shown below:
 - IP 10.0.0.1
 - IP Range 10.0.0.1-10.0.0.5
 - IP Subnet 10.0.0.0/24 or 10.0.0.0/255.255.255.0
 - Computer Name Home Computer
- Click the 'Add' button

Repeat the process to add more targets.

- Click 'Next' to continue.
- Login to the target device using either use the existing administrator credentials, or custom credentials.
- Next, choose one of the following scan types:
 - Quick Scan: Scans critical and commonly infected areas of target endpoints
 - Full Scan: Scans all files and folders on target endpoints.

By default, the IP subnet details are added in the network address field. The CFA tool will start discovering computers within the specified network, if the subnet details are given and then start the scanning process.

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool	_ 🗆 ×
2% Scan In Progress (Files: 1680 Computers: 0 of 115)	🕤 Previous Scans 🏾 Create Report 🍥 Options 🚺 Help
Image: Non-State Image: Non-State<	Stop Scan
Q Search by Computers	Group by 📮 📑
Name	Size Verdict 🔄
Iocalhost (127.0.0.1) 1680 files scanned (2.33%). Unknown: 0. Malici	ious: 3. In Analysis 17. In Progress
Please enter your email to receive a detailed scan results repor	t: customermail@enterprise.com Submit
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solut	tions. Visit one.comodo.com to learn how Comodo can help protect your environment.

Scan progress is shown for each computer. Overall progress is shown on the title bar.

- Stop Scan Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:

COMODO Fo	orensic Analysis To	ol				_ 🗆 ×
Scan Completed (Files: 35260 Compute	rs: 1 of 1)	9	Previous Scans	i Create Repo	rt 🍥 Options 🚺 Help
	۵	G	۵			New Custom Scan
35218 (99.88%) Clean Files	30 (0.09%) Malicious Files	3 (0.01%) Not Analyzed	9 (0.03%) In Analysis			Start Discovery
Watch of Comodo Free that you re Comodo A and reporti unknown fit use such ur	ut! Malware Is Def prensic Analysis has scann consider your current sect dvanced Endpoint Protect ng capabilities. It follows les inside a secure contain known files with no impa	ected! ed your environment urity posture to elimi ion keeps your endp "Default Deny" postu rer until a definitive v ct to the usability and	and detected m nate the danger of coints free from n re which allows k erdict of "good" d yet no harm to	alware on one or mo of infecting your end nalware now and in t mown files to freely r or "bad" is delivered the system.	re of the systems. We points. the future and provider run, blocks bad files an . Comodo Auto-Contai	recommend s essential management d automatically launches inment™ feature allows to
Please	enter your email to receiv	e a detailed scan resu	ults report: cust	tomermail@enterp	rise.com	Submit

Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit one.comodo.com to learn how Comodo can help protect your environment.

COMODO Creating Trust Online*

- There are two ways you can view the results:
 - **Group by Computer**: Shows each computer on a separate row. Expand any row to view unknown files found on that computer.
 - **Group by File**: Shows each unknown file on a separate row. Expand any row to view the endpoints on which the file was found.
- Detailed Scan Results Receive a report from Comodo Valkyrie about the unknown files on your network.
 Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.
 - Enter your email address in the field at the bottom
 - Click 'Submit' to receive the report at the address you supplied.

VALKYRIE					SIGN IN .
Forensic Analysis T	ool Scan Results				
FORENSIC ANALYSIS S Show 25 entries File Name #	Path	SHA1 0	S Last Activity 👻	earch: Final Verdict 🎙	Human Ex
yoga.dll	c:\program files\windo	16a7e57546a6f1c83a5	2019-02-22 15:07:19	In Queue	Not Ready
skypeproxiesandstubs.dll	c:\program files\windo	cbd20af3001d36b95d5	2019-02-22 15:07:18	In Queue	Not Ready
chakrabridge.dll	c:\program files\windo	1af202ca17cc81c6029	2019-02-22 15:07:17	In Queue	Not Ready
skypeapp.dll	c:\program files\windo	45f9e25557117928669	2019-02-22 15:07:17	In Queue	Not Ready

Valkyrie results will be displayed in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

Refer to the section 'Scan Results' for more details.

3.4 Scan your Local Computer

The local computer options lets you scan files, folders and drives on the computer you are using.

Click 'Custom Scan' on the home screen to open the scan wizard:

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool	_ 🗆 ×
Discovery Completed	🕞 Previous Scans 🐽 Create Report 🔞 Options 🕧 Help
34 Devices Found	Scan Now Custom Scan
Q Search by Computers	10
 None 10.108.51.10 	10.108.51.19
🔲 💂 Win10	10.108.51.12
	10 108 51 36
Start Scan Wizard	*
Select Scan Targets	
Como	Network Addresses Scan computers by specifying IP addresses or endpoint names
+ Workgroup Scan computers by selecting them from Workgroup	This Computer Scan this computer
	Cancel

Click 'This Computer'

COMODO Creating Trust Online*

Start Scan Wizard	×
Select Scan Targets	
+ Active Directory Scan computers by selecting them from Active Directory	Network Addresses Scan computers by specifying IP addresses or endpoint names
+ Workgroup Scan computers by selecting them from Workgroup	This Computer Scan this computer
	Cancel

The three scan types will open.



- Select the endpoints that you want to scan and choose one of the following scan types:
 - Quick Scan: Scan critical and commonly infected areas of your computer.
 - Full Scan: Scan all files and folders on your computer.
 - Custom Scan: Scan selected files or folders.

If you choose the 'Quick' or 'Full Scan' options then the scan will begin immediately. If you select 'Custom Scan', then you first choose the directories and files you want to scan:

Start Scan Wiz	zard	×
	Select Directories	
	▲ 💌 C:\	
	SRecycle.Bin	
	SWINDOWS.~BT	
	Documents and Settings	
	OpenSSL-Win32	
	PerfLogs	
	Program Files	
	Program Files (x86)	
	ProgramData	
	Recovery	
	Scan critical areas of computer which are most often targeted by malware	
Back	Scan	

- Select 'Scan critical areas...' to scan frequently targeted areas of your computer in addition to the items in your custom scan.
- Click 'Scan' to begin the scan.

COMODO Creating Trust Online*

OMODO Forensic Analysis Tool				_ 🗆 ×
38% Scan In Progress (Files: 0 Computers: 0 of 29)	🕞 Previous Scans	(d) Create Report	Option	ns 🚺 Help
			Stop Scar	n
Name		Size Ve	rdict	
10.108.51.10 (10.108.51.10) Unknown error		Fai	led	
Win10 (10.108.51.12) Login problem: invalid username or bad p	password.	Fai	led	
calltransfer044 (10.108.51.36) Unknown error		Fai	led	
😥 seo014 (10.108.51.53) Unknown error		Fai	led	ß
Iead03.ch.office.comodo.net (10.108.51.54) Unknown error		Fai	led	
SEO001 (10.108.51.56) Unknown error		Fai	led	
seo003.ch.office.comodo.net (10.108.51.58) Connecting to the	e target computer	In	Progress	
SE0005 (10.108.51.60) Connecting to the target computer_		In	Progress	
When all the files are analyzed, you will receive a detail	led report at comodo1@yopma	il.com	Edit I	Email

Scan progress is shown at the top of the interface.

- Stop Scan Discontinue the scan process.
- Results are shown in the CFA interface at the end of the scan. All unknown files are uploaded to Valkyrie for further testing:

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool	_ 🗆 ×
Scan Completed (Files: 1349 Computers: 1 of 1)	Previous Scans 🐽 Create Report 🍥 Options 🧃 Help
1362 (100%) Clean Files	New Custom Scan Detailed Scan Results Start Discovery
Rest Assured Your Endpoints Are Clean from Malware! Concratulational Comodo Ecrensic Applysis has scanned your environment at	nd detected no malicious or unknown files. However
unknown files containing malware with previously unknown exploits can ente	r any time unnoticed.
Comodo Advanced Endpoint Protection keeps your endpoints free from mal and reporting capabilities. It follows "Default Deny" posture which allows kno unknown files inside a secure container until a definitive verdict of "good" or use such unknown files with no impact to the usability and yet no harm to the	ware now and in the future and provides essential management wn files to freely run, blocks bad files and automatically launches "bad" is delivered. Comodo Auto-Containment™ feature allows to e system.
When all the files are analyzed, you will receive a detailed report at o	pmodo1@yopmail.com Edit Email
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security solutions. Visit	one.comodo.com to learn how Comodo can help protect your environment.

· The results interface contains details of each scan you have run along with verdicts for each file discovered

OMODO Forensic Analysis Tool			_ 🗆 ×
Scan Completed (Files: 1349 Computers: 1 of 1)	Previous Scans	🐽 Create Re	port 🍥 Options 🚺 Hel
1349 (100%)			Image: New Custom Scan Detailed Scan Results
Clean Files Q. Search by Files		_	Group by
Name Ref: Skypeapp.exe (Microsoft Skype) 1 instance.		Size 21 KB	Clean
🖅 🚡 skypeapp.dll (Microsoft Skype) 1 instance.		24 MB	Clean
🛨 👸 winstore.app.exe (Windows Store) 1 instance.		16 KB	Clean
🛨 🛅 photosapp.windows.dll 1 instance.		13 MB	Clean
🛞 📸 winstore.app.dll (Windows Store) 1 instance.		30 MB	Clean
🗄 🛅 microsoft.photos.exe 1 instance.		470 KB	Clean
🛨 🛅 mediaenginecswrapper.dll 1 instance.		3 MB	Clean
When all the files are analyzed, you will receive a detai	ed report at comodo1@yopma	iil.com	Edit Email
When all the files are analyzed, you will receive a detai	ed report at comodo1@yopma	to learn how Come	do

Comodo Forensic Analysis Admin Guide | © 2019 Comodo Security Solutions Inc. | All rights reserved.

COMODO Creating Trust Online

Detailed Scan Results – Receive a report from Comodo Valkyrie about the unknown files on your network. Valkyrie is a file verdict service which inspects unknown files with a range of static and dynamic tests.

Enter your email address in the field at the bottom

Click 'Submit' to receive the report at the address you supplied.

VALKYRIE				SIGN IN 🗲
Forensic Analysis Tool Scan Res	sults			
FORENSIC ANALYSIS SCAN SESSION D Show 25 v entries	ETAILS		Search:	
File Name 🕴 Path 🌵 SHA1 🌵 Last Activit	ty 🔻 Final Verdict 🌢	Human Expert Verdict 🖗	Human Expert Analys	is Status 🕴
	No	data available in table		
<				>
No entries found				< >

When your computer is free of unknown files, you will not find any data when you click the 'Detailed Scan Results' button.

Valkyrie results are shown in the Valkyrie portal. Existing Valkyrie users can login by entering their Comodo username/password or Valkyrie license number. If you do not have a license, click 'Sign Up' on the right to create a free account.

4 Scan Results

- Scan results are automatically shown in the CFA interface after a scan finishes.
- The scan checks the reputation of each file against Comodo's file-lookup service, a huge database of blacklisted and white-listed files.
- Blacklisted files are flagged as malicious and should be deleted or quarantined. White-listed files are safe to
 run.
- If a file is not on either the blacklist or whitelist, then it is categorized as 'unknown'. Unknown files are
 automatically submitted to Comodo Valkyrie where they will undergo a range of static and dynamic
 behavioral tests to discover whether they are malicious or not.
- The CFA interface displays results of both files analyzed by Forensic Analysis and Valkyrie analysis:

COMODO Creating Trust Online*

ican Completed (F	iles: 58864 Computer	s: 2 of 7)	🕤 Previo	ous Scans 🏾 👜 Cre	ate Report) Options 🕧 H
58703 (99.73%) Clean Files	5 (0.01%) Malicious Files	94 (0.16%) Unknown Files	11 (0.02%) Failed	6 51 (0.09%) In Analysis	• •	New Custom Scan Detailed Scan Results Start Discovery
Q Search By Compute	5					Group By 📮 🗐
Name					Size	Verdict
🗄 🧕 DESKTOP-TTP	O9PR (10.108.51.100)	Completed: Total scanned: 3	33350. Unknown: 1	0. Malicious: 4. In An		Completed
P TONYSTARK-F	PC (10.108.51.245) Logir	n problem: invalid usernam	e or bad password	L.		Failed
🛞 🧐 WIN-CU2OX8	JDY3D (10.108.51.129)	Completed: Total scanned:	25521. Unknown:	84. Malicious: 1. In A		Completed
DESKTOP-1A	MD5C1 (10.108.51.104)	This computer is not acces	sible.			Offline
SKYHIGH-PC	(10.108.51.192) This con	nputer is not accessible.				Offline
TOM (10.108.	51.175) This computer is	not accessible.				Offline
WIN-8719G19	COH7 (10.108.51.117) 1	his computer is not access	ible.			Offline
Diease e	nter your email to receive	a detailed scan results ren	ort customer	ail@enternrise.com		Submit

- Scan results are listed for each computer. Each row has a quick summary of the scan results, including total files scanned and how many were malicious or unknown.
- Click the plus symbol beside an endpoint to view unknown and malicious files detected by the scan.
- Click the icons next to 'Group By' to view results by 'Computer' or by 'Files'. Group By 📃 📠
- Expand an endpoint's results then click the 'Name', 'Size' or 'Verdict' column headers to sort files in order of the column name.
- To search for a particular endpoint, enter its name or IP address in the 'Search' box at the top right. Clear the search box to display all endpoints again.
- Click the funnel icon on the right is to filter endpoints by scan status:



- In Progress Endpoints which have a scan currently running
- Canceled Endpoints on which a scan was aborted
- · Completed -Endpoints on which a scan has successfully finished

COMODO Creating Trust Online*

- Failed Endpoints on which CFA was unable to complete a scan
- · Offline Endpoints which are not responding at this time
- If the filter icon is blue
 again.

then filter(s) are applied. Click 'Clear Filter' to display all endpoints

Unknown files are uploaded to Valkyrie for analysis. You can view the results of the Valkyrie analysis by clicking the 'Detailed Scan Results' button. This will open the Valkyrie results page:

VALKYRIE				l	SIGN II
Forensic Analysis Tool S	ican Results				
FORENSIC ANALYSIS SCAN S Show 25 v entries	ESSION DETAILS		Search:		
File Name 💧	Path 🍵	SHA1 A			
		JHAT	Last Activity 👻	Final Verdict 🖗	Hur
9CEBCF06E53458AD826B6336	\\127.0.0.1\C:\Window	713f318f4405fbc1b30a	2019-02-25 18:14:06	Final Verdict 🖗	Hur Clea
9CEBCF06E53458AD826B6336 D5DD57BEAAE521AFDC067C6	\\127.0.0.1\C:\Window	713f318f4405fbc1b30a	Last Activity 2019-02-25 18:14:06 2019-02-25 18:14:05	Final Verdict 🖗 Clean Clean	Hur Clea Clea
9CEBCF06E53458AD826B6336 DSDD57BEAAE521AFDC067C6 ED58CE97E4A9395A0C2075C9	\\127.0.0.1\C:\Window \\127.0.0.1\C:\Window C:\Windows.old\Users\	713f318f4405fbc1b30a cffb01b357a8b602aba 28f0d8c8650d6ed149e	Last Activity 2019-02-25 18:14:06 2019-02-25 18:14:05 2019-02-25 18:14:04	Final Verdict Clean Clean Clean	Hur Clea Clea Clea

Valkyrie Detailed Analysis Results - Table of Column Descriptions				
Column Header	Description			
File Name	The name of the submitted file			
Path	The IP of the endpoint and the file's path details			
SHA1	The SHA1 hash value of the file.			
Last Activity	The date and time the last activity of analysis was performed.			
Final Verdict	 The Valkyrie dynamic and static analysis results for the file. The results available are: Clean - The file is safe to run No Threat Found - No malware found in the file, but cannot say it is safe to run Malware - The file is a malware and should not be run 			
Human Expert Verdict	The results of the file after Human expert analysis: • Clean - File is safe to run			

COMODO Creating Trust Online

Comodo Forensic Analysis - Admin Guide

	Malware - The file is a malware file					
	 Potentially Unwanted Application (PUA) - Applications such as Adware, Spyware and so on 					
	No Threat Found - No malware found in the file, but cannot say it is safe to run					
	Not Ready - Indicates manual analysis of the file is in progress					
Human Expert	Indicates the status of files submitted for Human Expert analysis. The statuses are:					
Analysis Status	In Queue - The analysis has not started					
	 In Progress - The analysis has started and in progress 					
	 Analysis Completed - The analysis is completed and verdict displayed under the 'Manual Verdict' column 					
	• Objected - Indicates the user wants a re-analysis of the file. If the user thinks that the initial manual verdict for the file is wrong, he/she can submit it again for another manual analysis.					
	Objection Completed - Indicates the manual re-analysis is completed.					
Request Type	Indicates the type of input given to receive Valkyrie results.					
	Queried - The file were automatically uploaded to Valkyrie					
	Manual - The files were manually uploaded to Valkyrie					
Actions	The available actions are:					
	• View Info - You can view the complete details of the results for the file such as summary, static analysis, dynamic analysis and file details.					
	- Download Automatic Analysis Report - Allows you to download the report in PDF format.					
	- View Virus Total Result - Takes you to the Virus Total website that displays its results for the file.					
	- Send to Manual Analysis - Allows you to submit the file for manual analysis by Comodo technicians.					

You can also view detailed Valkyrie results in the reports area. See Reports for more details.

5

Discover Computers

- The software starts to discover all computers on your local network when you first launch the tool.
- You can skip discovery if you do not want to scan local machines.

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool	_ 🗆 ×
60% Searching for Available Devices	🕞 Previous Scans 👍 Create Report 🍥 Options 🧃 Help
23 Devices Found	Skip Discovery
Q Search by Computers	
Name	IP
. 10.108.51.10	10.108.51.10
🔲 🚂 Win10	10.108.51.12
Calltransfer044	10.108.51.36
seo014	10.108.51.53
🔲 📮 SEC004	10.108.51.54
🔲 💂 SEO001	10.108.51.56
🗌 🖵 Seo003	10.108.51.58
🔲 🖳 SEO005	10.108.51.60
	"Activate Windows
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of securit	y solutions. Visit <u>one.comodo.com</u> to learn how Comodo can help protect your environment.

All discovered computers are shown in the results screen. You can now scan these machines for unknown files:

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool	▶ _ □ ×
Discovery Completed	🕤 Previous Scans 👜 Create Report 🎯 Options () Help
34 Devices Found	Scan Now Custom Scan
Q Search by Computers	
I Name	Ib
10.108.51.10	10.108.51.10
🔲 💂 Win10	10.108.51.12
calltransfer044	10.108.51.36
seo014	10.108.51.53
SE0004	10.108.51.54
E SECO01	10.108.51.56
Seo003	10.108.51.58
E George Secons	10.108.51.60
	10.000.22.41
Comodo Forensic Analysis Tool is part of the Comodo ONE portfolio of security soluti	ons. Visit one.comodo.com to learn how Comodo can help protect your environment.

6 Reports

There are three types of report you can order:

- Executive report An overall report which shows the scope of the scan, the number of devices scanned, the number of unknown programs found and more.
- Per device report Groups the results by computer. Details how many trusted programs, unknown programs and malicious programs were found on specific machines.
- Per program report Shows the impact of a file on your network. Shows the names and IP addresses of the devices on which the file was found.

COMODO Creating Trust Online*

COMODO Forensic Analysis Tool			_ 🗆 ×
Scan Completed (Files: 1359 Computers: 1 of 1)	Previous Scans	(in) Create Report) Options (j) Help
1359 (100%) Clean Files		Executive Report Per-Device Report Per-Program Repor	New Custom Scan Detailed Scan Results
Q Search by Computers Name		Size N	Group by
 Completed: Total files windows apps \microsoft.skypeapp_14.39.222.0_ C\program files \windows apps \microsoft.windows store_11811.1 	x64_kzf8qxf38zg5c\skypeba x64_kzf8qxf38zg5c\skypeba	178 КВ (276 КВ (Clean Clean
When all the files are analyzed, you will receive a detailed	report at comodo1@yopms utions. Visit one.comodo.com	il.com to learn how Comodo ca	Edit Email

Refer to the following sections for more details:

- Executive Report
- Device Report
- Program Report

6.1 Executive Report

Create Report) Options 🕧
Executive Report	
Per-Device Report	New Custom Scan
Per-Program Report	Detailed Scan Results
ļ.	Start Discovery
	Create Report Executive Report Per-Device Report Per-Program Report

Click 'Reports' and then 'Executive Report':

COMODO Creating Trust Online*

The report will be generated and displayed:



Scroll down to view the full report. You can save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file name and save in another location.

- Report Summary General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- Summary Charts Details of programs found on scanned devices and the overall file rating of scanned devices.
 - Scanned Devices File Rating Chart showing the trust rating of programs discovered on scanned devices. Shows the percentage of trusted programs, unknown programs, malicious programs, and programs for which analysis is still in progress.
 - **Device Assessment** Pie chart which shows the percentage of devices that are safe, infected, at risk and not yet scanned.

6.2 Device Report

The 'Per Device Report' shows the trust rating of files on each device scanned. It includes details of malicious items found on each device, unknown files found, files that are still in-analysis and the path of files.

• Click 'Reports' then 'Per Device Report'.

The report will be generated and displayed:

COMODO Creating Trust Online*



Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

- **Report Summary** General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- Summary Chart Bar chart showing the top 10 endpoints that contain unknown/malware files.
- **Details per Device** Inventory of files discovered on each endpoint. This includes the name of the device, quantity of malicious/unknown files, the path of each malicious/unknown file and more.

6.3 Program Report

The 'Per Program Report' shows the footprint of each file analyzed by Valkyrie. This includes details of each malicious/unknown file found, the devices on which they were found, the path of the files and more.

Click 'Reports' then click 'Per Program Report'.

The report will be generated and displayed:

COMODO Creating Trust Online*

Per-Program	n Report		
	1 /1	Search	
	COM030	Eorensic Analysis Tool	
	COMODO		
	Forensic Analysis		
	Per-Program Report	2/28/2019 2:42:24 PM	
	Devent Commence		
	Report Summary		
	Device Source:	Local Computer (localhost)	
	Scan Started:	2/28/2019 1:31:03 PM	
	Scan Finished:	2/28/2019 1:39:19 PM	
	Inaccessible Devices:	0	
	Scan Attempts:	1	
	Successful Scans:	1	
	Failed Scans:	0	
	Total Files Scanned:	1359	
	Trusted Files Found:	1359	

Scroll down to view the full report. Note - please save the report if you wish to keep it for further reference. The report will not be available in the interface after the application is closed. To save the report, click the folder icon at the top-left, copy the report file and save in another location.

- **Report Summary** General scan details, including the number of devices scanned, date and time of the scan, number of malware found and so on.
- Summary Chart Shows the top 10 unknown/malicious programs in bar graph.
- **Details per Program** Granular report showing the impact of each analyzed file on your network. This includes the names and IP addresses of the devices on which it was found on and the overall trust rating of the program.

7 About Comodo Forensic Analysis

The 'About' dialog show product information and version number.

• Click 'Help' > 'About':

COMODO Creating Trust Online*

COMODO Fo	rensic Analysis Tool					-	_ 🗆	×
Scan Completed (iles: 1359 Computers: 1	of 1)	Previous So	ans 🌰 Creat	e Repor	t 🍥 Options	()	Help
1359 (100%) Clean Files Search by Compu- Name Localhost (1)	About 4			×		Abou	t Requir an Resul wery	ements
🔂 c\prog	© 2017 Comodo Security Se	Creating Trust Online roduct Name: roduct Version: olutions, Inc. All Rights F	Forensic Analysis Tool 4.0.30606.102 leserved.	Close	KB	Clean Clean		
wł Comodo Forensic Analysis To	en all the files are analyzed, y ol is part of the Comodo ON	you will receive a detail E portfolio of security s	ed report at comodo1@y plutions. Visit <u>one.comode</u>	opmail.com	Comodo	Edit Ei can help protect yo	mail ur enviro	Donment.

- Product Name The full name of the product
- Product Version The version number of the product
- Click the 'Close' button to return to the application.

COMODO Creating Trust Online

8 Agent Requirements

The 'Agent requirements' window contains advice to help you run scans successfully.

• Click 'Help' > 'Agent Requirements':

сомод	O Fo	orensic Analysis Tool	_	. 🗆 ×
Scan Comp	oleted (Files: 1359 Computers: 1 of 1)	Options	() Help
1359 (10 Clean F	00%) Files		About Nr Agent Detailed Sca Start Discov	Requirements n Results ery
Q Search I	Age	nt Requirements	roup by	26
Name	Ø	Check whether a target computer is turned on and connected to the network.	t	
مترينيا التا ال	Ø	Check whether firewall on a target computer is turned Off.	eted	
E	Ø	Check whether IP address of a target computer is correct.		
	Ø	In the Network Neighbourhood run Network Wizard, enable file sharing.		
	Ø	Make sure Administrator password is not blank and correct.		
	Ø	Check whether 'Forceguest' option on target computer is disabled: HKLM\\SYSTEM\ \CurrentControlSet\\Control\\Lsa 'forceguest' dword is 0.		
Comodo Forensic /	Ø	If the account is not a built-in Administrator, check whether: HKLM\\SOFTWARE\\Microsoft\ \Windows\\CurrentVersion\\Policies\\System 'LocalAccountTokenFilterPolicy' dword is 1. Close The second of the Comodo ONE portfolio of security solutions. Visit one comodo com to learn how Comodo can bell	Edit En	iail Mindows.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street Clifton, NJ 07013 United States Tel : +1.877.712.1309 Tel : +1.888.551.1531 https://www.comodo.com Email: EnterpriseSolutions@Comodo.com