

### **DIGITAL FORENSIC PROJECT**



### DISCLAIMER



This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.







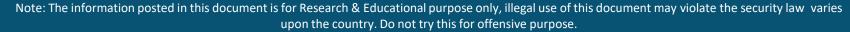
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

**Project Name:** Remote Imaging of A system

**Tool Used:** Belka Soft Evidence Center

#### **Platform:** Windows

Image: Image	PEvidence Center Trial 9.9800.6405 x64		_ = =	×
C bashord       C bashord () C bashord () () That Manager () That Manager () () That Manager () That Manager () () That Mana	File View Tools Help			
Construction				
Construction				
New case Bot folder: CuterxNousdAppDataReamingSeliasoftExidence Center     Cose plane: CuterxNousdAppDataReamingSeliasoftExidence CenterReamote.System.imagna     Investigation: Tutera center     Periode: Tutera center     Bott influer: CuterxNousdAppDataReamingSeliasoftExidence CenterReamote.System.imagna     Investigation:     Investigation: <td>Dashboard 🔁 Case Explorer 🗵</td> <td>Overview 🗷 😫 Timeline</td> <td>🕱 🕅 Bookmarks 🗵 🖉 File System 🕱 🗸 Task Manager 📧 🖳 Remote Acquisition 📧 🖉 G Incident Investigations 💌</td> <td>-</td>	Dashboard 🔁 Case Explorer 🗵	Overview 🗷 😫 Timeline	🕱 🕅 Bookmarks 🗵 🖉 File System 🕱 🗸 Task Manager 📧 🖳 Remote Acquisition 📧 🖉 G Incident Investigations 💌	-
Dot Note::       Controls::       Control::       Controls::       Control::       Contro::       Control::       Control:: </td <td></td> <td>Case <u>n</u>ame:</td> <td>Remote-System-Imaging</td> <td></td>		Case <u>n</u> ame:	Remote-System-Imaging	
Image: Second	New case	<u>R</u> oot folder:	C:\Users\Yousuf\AppData\Roaming\Belkasoft\Evidence Center	
Image: With Control Ling and Control Ling a	Cpen existing	Case <u>f</u> older:	C:\Users\Yousuf\AppData\Roaming\Belkasoft\Evidence Center\Remote-System-Imaging	1
Infe cone:         (UTC=0500) (Islamabad, Karachi         *           Recent cases         gescription:         *	Options	Investigator:	Yousuf & Shafi	]
Remote Imaging       Excretion         Cubern/Vouur/AppOstal_Memote Imaging)       Imaging         Imaging Cubern/Vouur/AppOstal_Memote Imaging)       Imaging Cubern/Vouur/AppOstal_Memote Imaging)         Imaging Cuber		Time zone:	(UTC+05:00) Islamabad, Karachi	
C:\Users\Yousuf\AppDiats\.Remote Imaging\		Description:		
Create and open				11 1
	C.\Users\Tousur\AppData\\Remote Tmaging\			
			<u>Create and open</u>	
elcome to Evidence Center Trial x64	Welcome to Evidence Center Trial x64			4







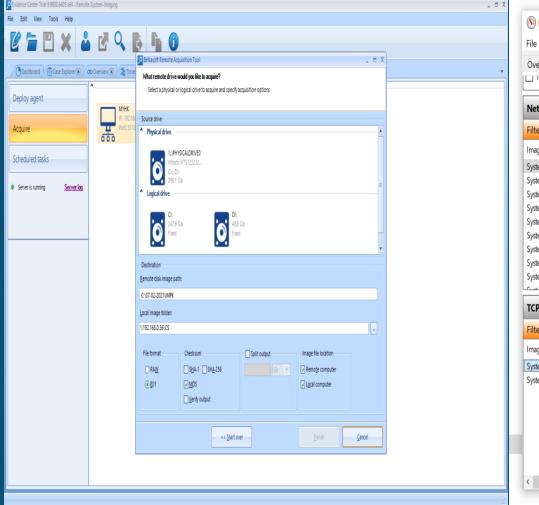
### **DESCRIPTION :**

The main objective is to acquire an image of a system remotely via an agent. Two (02) Windows 10 machine deployed. One Windows 10 machine act as a management server (Belka Soft Evidence Center 9.9) and Second windows 10 machines used for imaging.

🔎 Evidence Center Trial 9.9800.6405 x64 - Remote	ie-System-Imaging	_ @ X
File Edit View Tools Help		
🕒 Dashboard 🦯 🔁 Case Explorer 🗷 🗸 🤇	co Overview 🖹 🖉 Timeline 🗵 🔎 🖪 Options X Ions 🖹	
Deploy agent	Local deployment General Language Picture Video Carving VirusTotal Hashes Remote	<u>^</u>
	If you do not have a domain, you	
Acquire	Select a folder for the local install	
	192.168.000.057	
Scheduled tasks	Operating system Server gort:	
	© Windows Mac OS 6957	
Server is not running Server log	Generate WAN	
	Server IP address:	
	Remote GPO deployn	
	To install agent remotely, the proc Server gort:	
	Select network folder for remote in	
	Use SSL certificate	
	Generate	
	<u>S</u> L certificate file:	
	Remote WMI deployr	
	Enter folder for remote installation Password:	
	Computer name or IP: Schedule gownload start time:	
	3:20 PM ( )	
	Admin username:	
	Admin password:	
	000.000.000	
	Deploy IP port	
	0	v
		- the



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



		N	^	D-+		Torra -	c:
🔊 Resource	Monitor						- 🗆
ile Monito	or Help						
Overview C	PU Mem	nory Disk Network					
reams.exe	14052	۷ کار	1	5			
							<b>^</b>
Network Ac	tivity	1 Mbps Network	I/O	📕 0% Netw	ork Utilization	۲	Network
Filtered by Sy	/stem						
lmage	PID	Address	Send (B	/sec) Receive (B/s	Total (B/see	.) ^	
System	4	MYHK.bbrouter		464 176,519	176,983	3	
System	4	192.168.208.255		7 4	12	2	
System	4	192.168.16.255		7 4	12	2	W
System	4	192.168.0.255		4 4	9	9	60 Seconds
System	4	MYHK-IMPK.bbrouter		0 1	1	1	TCP Connections
System	4	239.255.255.250		113 0	113	3	
System	4	224.0.0.252		24 0	24	1	
System	4	52.114.133.68		11 0	11	1	
System	4	52.113.206.51		6 0	(	5	
C	4	F2 11 4 7C 222		r 0			
TCP Connec	ctions					۲	
Filtered by Sy	/stem						Ethernet
lmage	PID	Local Address	Local	Remote Address	Remot	Packet Loss ( La	
System	4	192.168.0.57	445	192.168.0.56	51102	0	
System	4	192.168.0.57	63974	192.168.0.56	445	0	
							Local Area Connectio





Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.