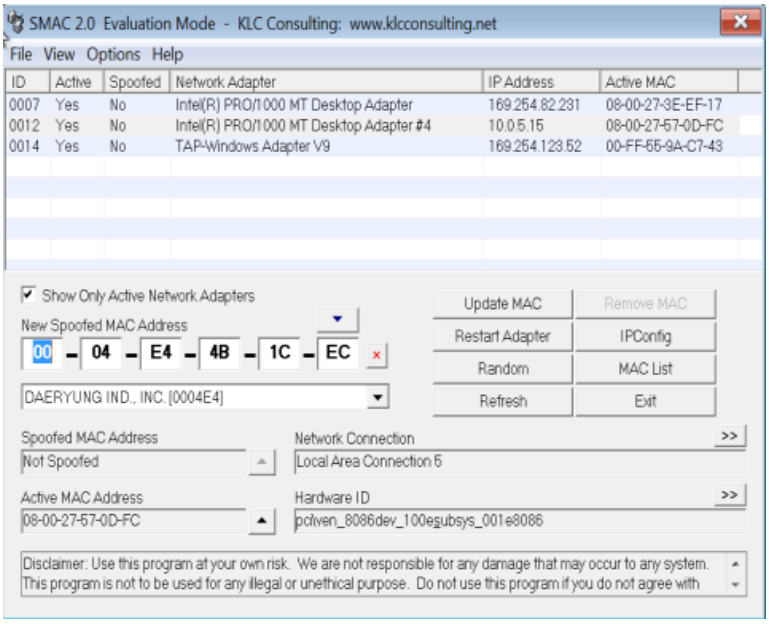
Sniffers
Lab Assignment (Module 8)

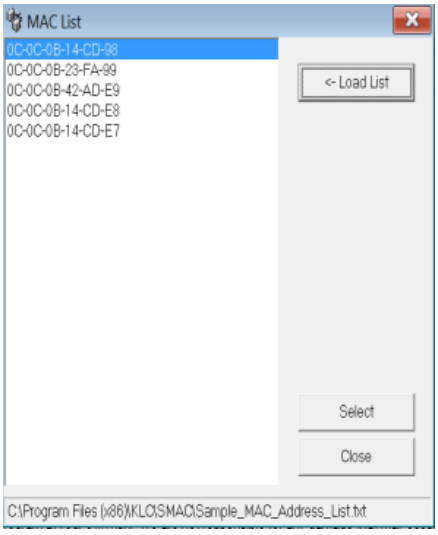
Name: Sachin Saj T K
Roll No: CB.EN.P2CEN18012
Date of Submission: 10/06/2019

Spoofing MAC Address Using SMAC

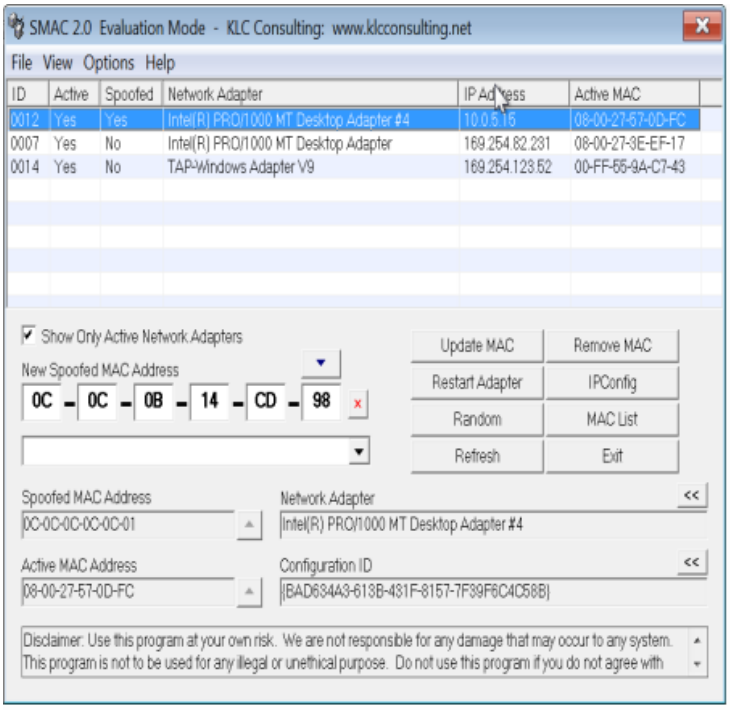
1. Smac



2. Loaded Mac list



3. Mac address spoofed

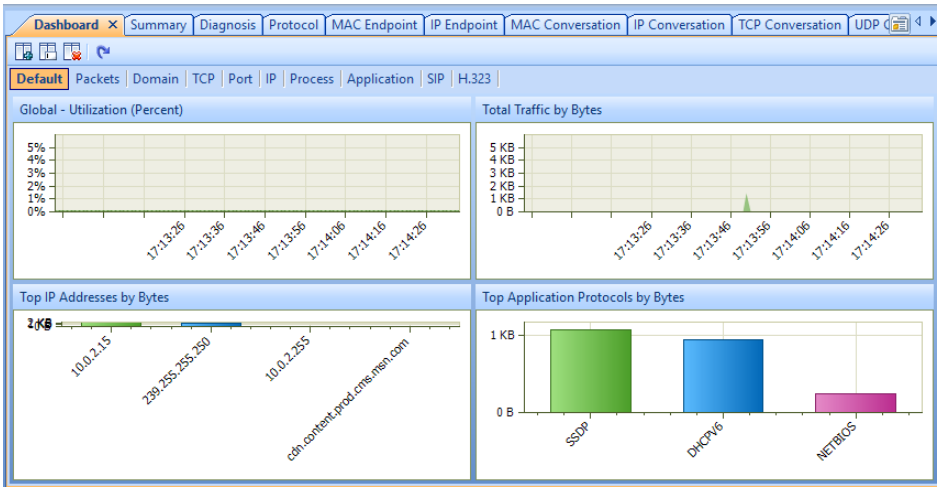


Lab Analysis

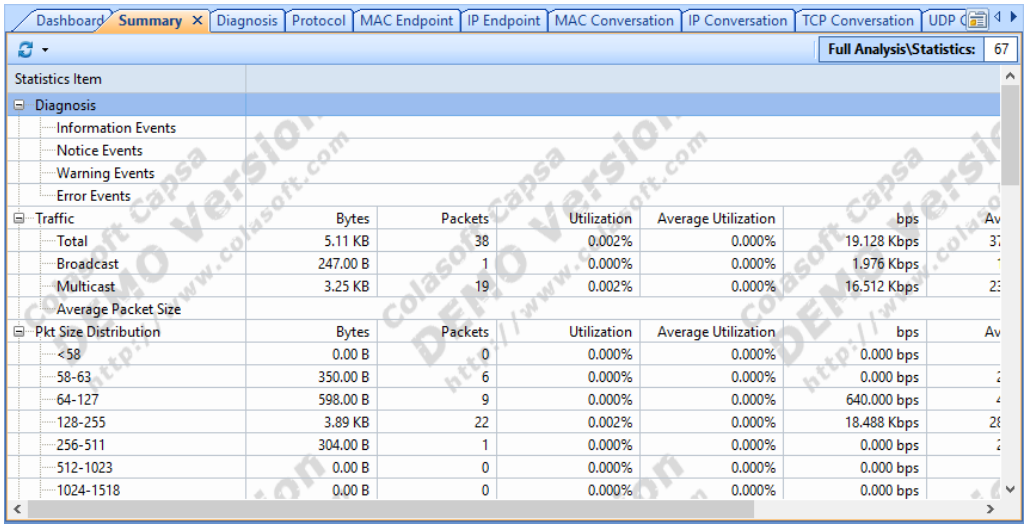
Tool/Utility	**Information Collected/Objective Achieved**
SMAC	**Host Name:** Intel® PRO/1000 MT Desktop Adapter #4 **Node Type:** nil **MAC Address:**08-00-27-57-0D-FC **IP Address:**10.0.5.15

Analyzing a Network Using the Capsa Network Analyzer

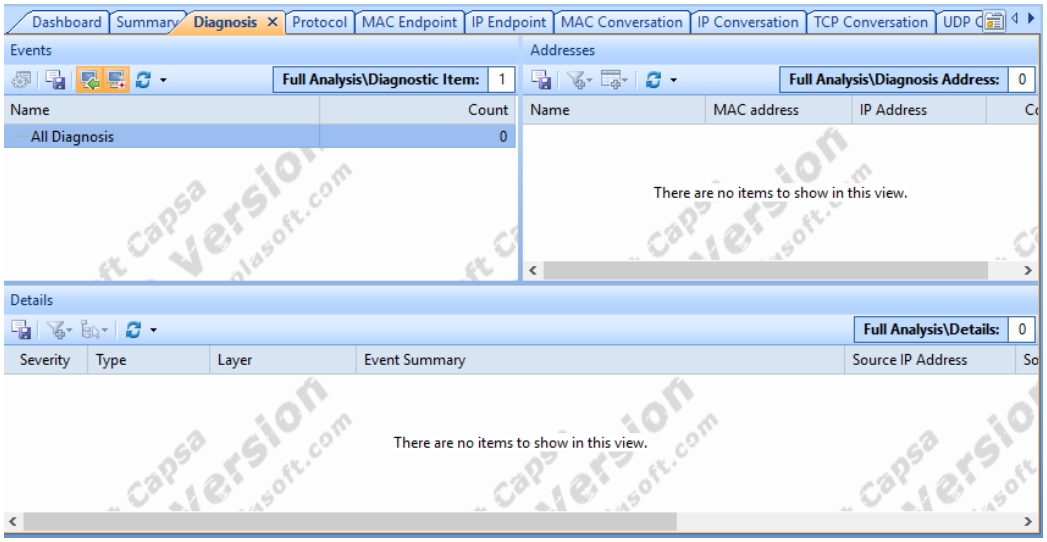
1. Dashboard



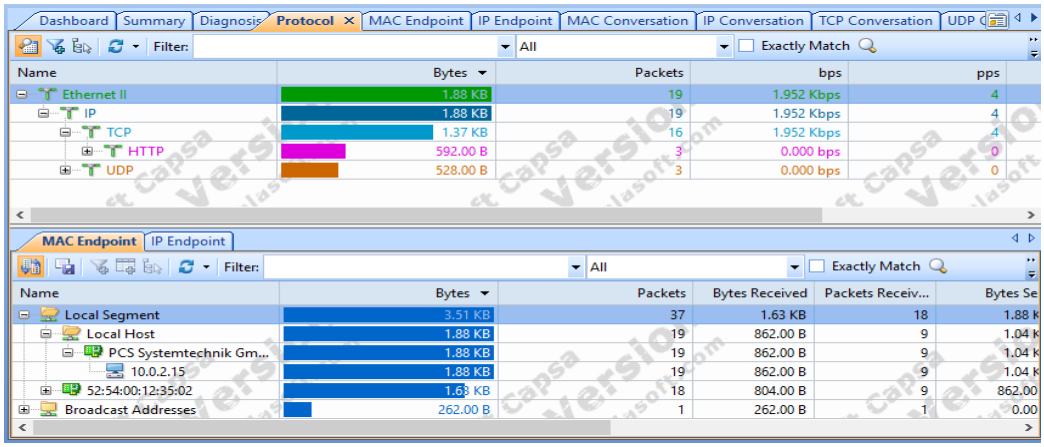
2. Summary



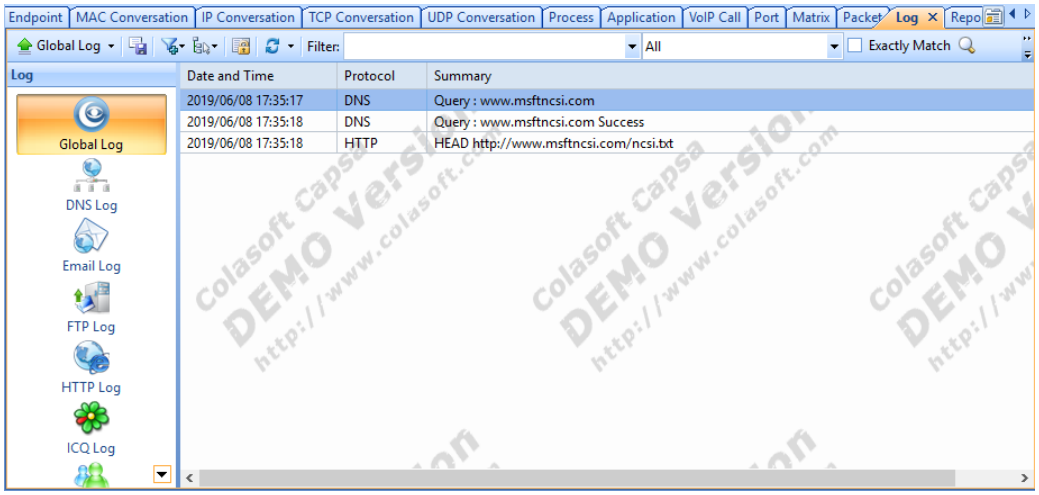
3. Diagnosis



4. Protocol



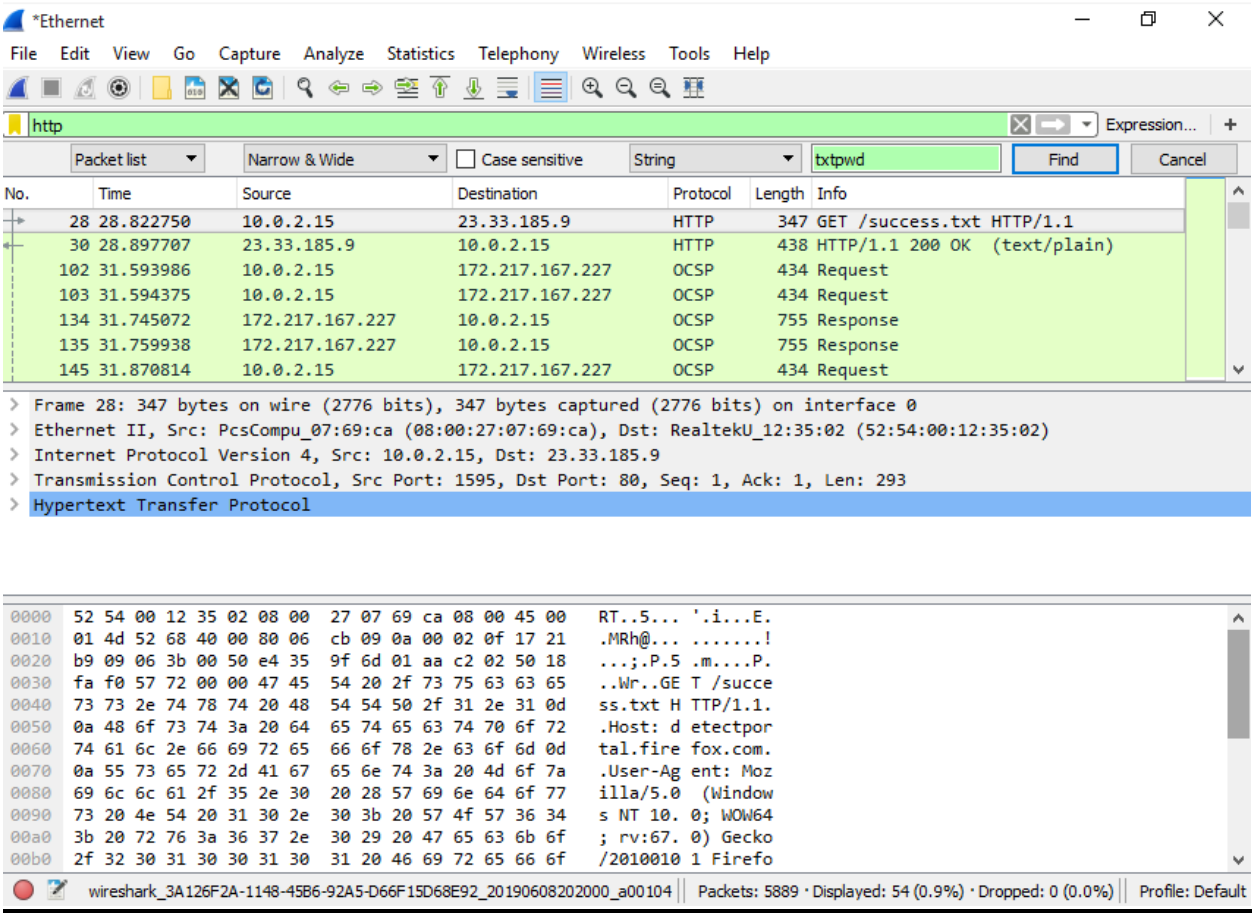
5. Logs



Tool/Utility	Information Collected/Objective Achieved
Capsa Network Analyzer	**Diagnosis:** • **Name:** nil • **Physical Address:** nil • **IP Address:** nil
	Packet Info: • **Packet Number**:7 • **Packet Length:** 80 • **Captured Length:** 76
	Ethernet Type: • **Destination Address:** 172.17.18.2:53 • **Source Address:** 10.0.2.15:65015 • **Protocol:** DNS_QUERY • **Physical Endpoint**: nil • **IP Endpoint:** 172.17.18.4
	Conversations: • **Physical Conversation:**10.0.2.15:59741 – 172.17.18.2.53 • **IP Conversation:** 10.0.2.15 – 172.17.18.4 • **TCP Conversation:** 10.0.2.15 – www.msftncsi.com • **UDP Conversation:** 10.0.2.15 – 172.17.18.4
	Logs: • **Global Log:** 2019/06/08 – DNS • **DNS Log:** 2019/06/08 -10.0.2.15 • **Email Log:** nil

	• **FTP Log**: nil • **HTTP Log:** nil • **MSN Log:** nil • **Yahoo Log**: nil

Sniffing Passwords Using Wireshark



Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
Wireshark	**Time:** 28.822750 **Source:**10.0.2.15 **Destination:** 23.33.185.9 **Protocol:** HTTP **Length:** 347 **Info:** GET/ success.txt HTTP/1.1