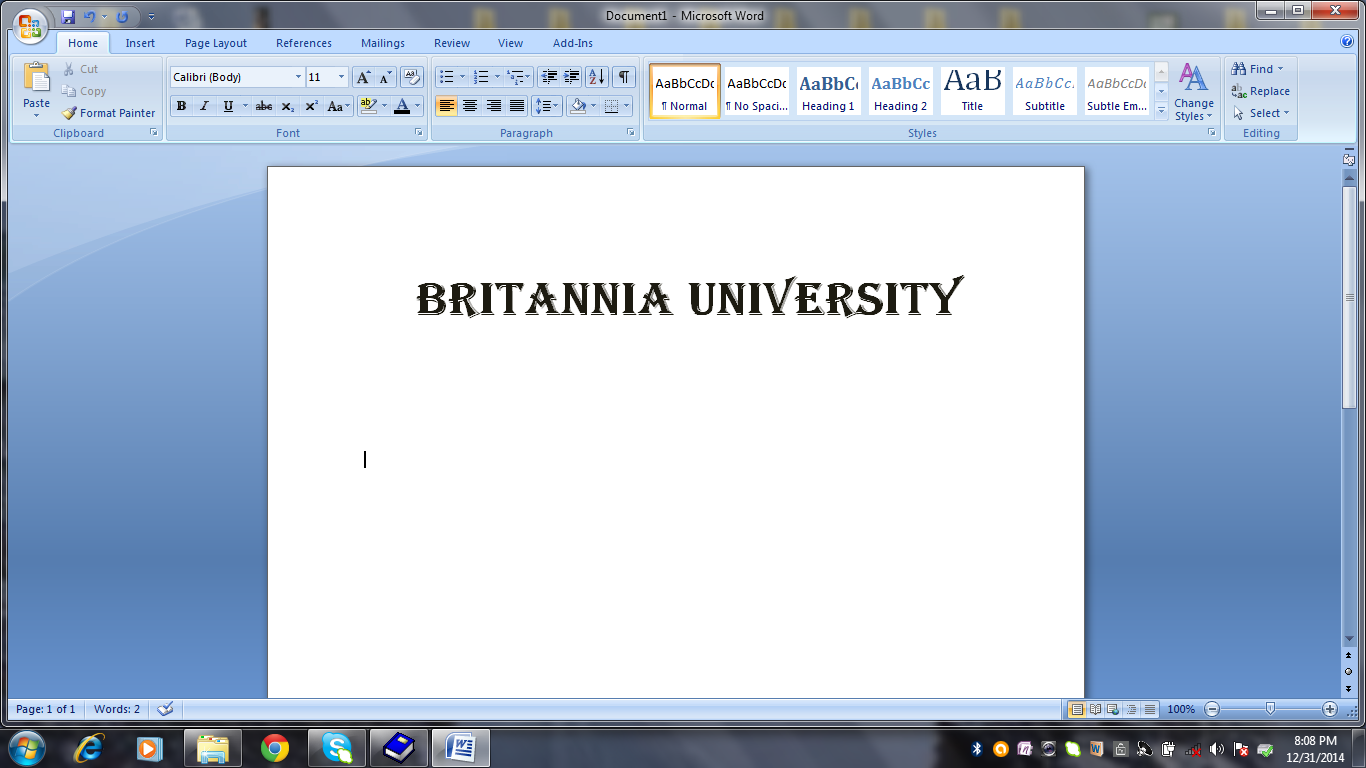
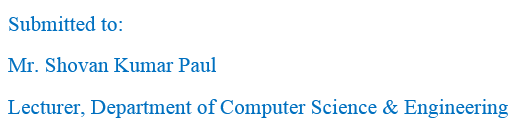


****

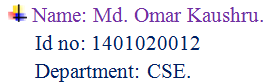
**Course title:** Network Security and Cryptography.

**Assignment on:**  Snort, openSSL, openSSH, openVPN, nMap.



Date of Submission: 4th January, 2017

Submitted by:

****

**Snort: Snort** is an open-source, free and lightweight network intrusion detection system (NIDS) software for Linux and Windows to detect emerging threats.

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

***OpenSSL:*** *OpenSSL* is a general purpose cryptography library that provides an open source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

***OpenSSH:*** *OpenSSH* (also known as OpenBSD Secure Shell) is a suite of security-related network-level utilities based on the Secure Shell (SSH) protocol, which help to secure network communications via the encryption of network traffic over multiple authentication methods and by providing secure tunneling capabilities.

***OpenVPN:*** *OpenVPN* is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

***Nmap:*** *Nmap* (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network.