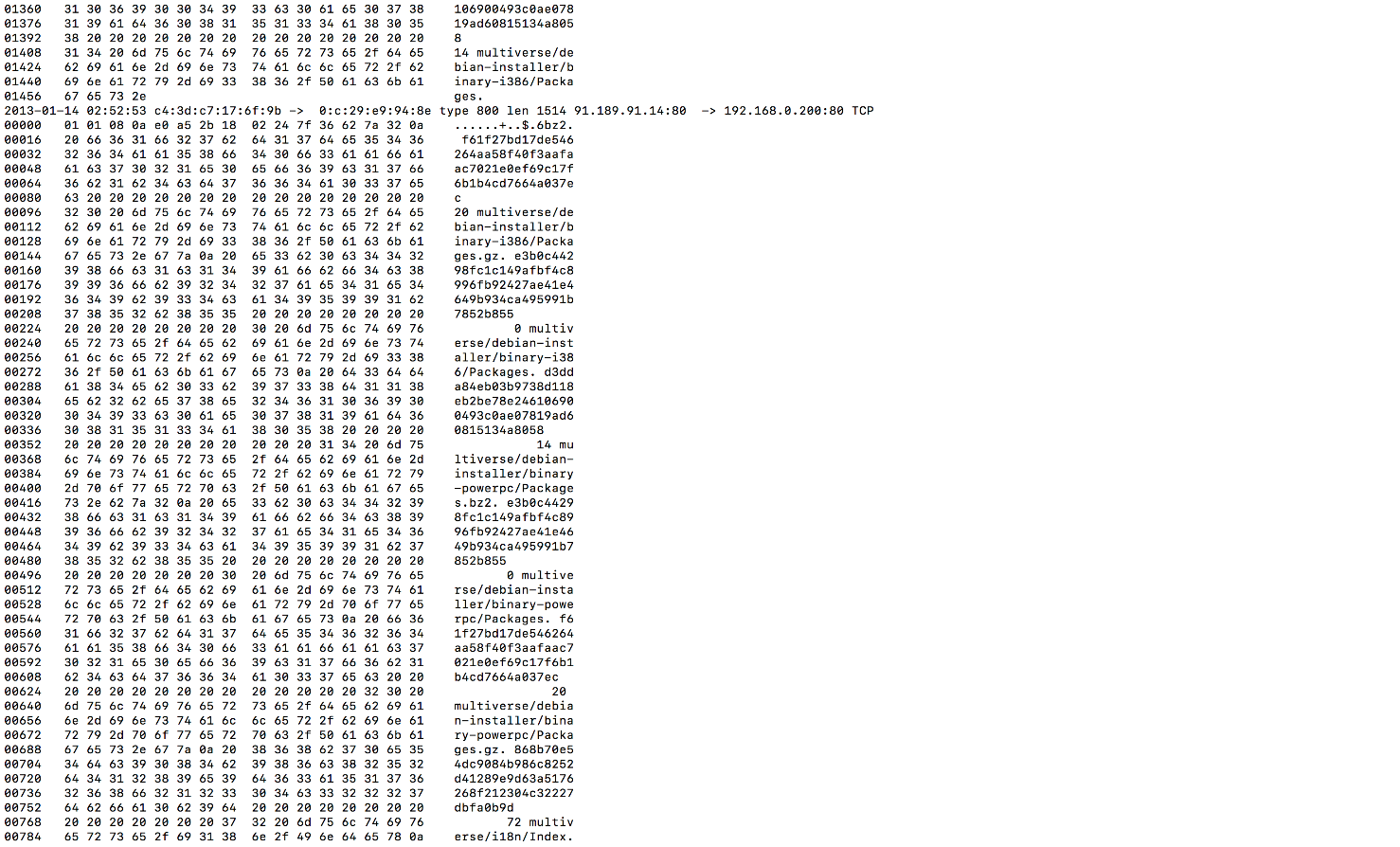
**Network Security Assignment 2 – Network Monitor**

**Introduction:**

I have created an application (mydump.c) which monitors the network of the device it runs on. If run without any command line arguments, it monitors the default device which is returned by the method (pcap\_lookupdev). We can pass an interface name by passing the interface-name as a Command line argument (CLA), preceded by -i. We can also read a pcap file by passing its name as a CLA preceded by -r. If we pass both -r and -i, -r will take precedence. We can also pass a filter expression, which will give us only those packets which are permitted by the filter expression. We can filter the packet on it’s payload using the CLA -s. All these CLA can be passed in any order and can be used independent of each other. An example of running this application will be:

**sudo ./mydump -r hw1.pcap ip proto** [**\\tcp**](file:///\\tcp) **-s binary**

It produces the following output.



**Output:**

The output columns are as follows:  
1. Date and time of the receipt of the packet

2. Source MAC address

3. Destination MAC address

4. Ether type of the packet

5. Packet length

6. Source IP address and port

7. Destination IP address and port

8. Protocol Name

9. Payload of the packet

**Code explanation:**

The following is a short explanation of the main crux of the code:

1. **Main**

* This function accepts input and then calls a function which infinitely monitors the packets
* It also calls the BPF filter if required

1. **processPacket**

* This function gets called whenever a packet is received by the Network card and it surpasses the filter
* This function then checks if the payload contains the required string (passed by -s) if any and grabs required information of the packet

1. **Print\_payload**

* This function prints the payload of the received packet

**Referrences:**

I have referred the following links for implementing this application:

* <http://www.tcpdump.org/pcap.html>
* <http://www.tcpdump.org/sniffex.c>
* Resources on <http://www.tcpdump.org/>
* <http://www.programming-pcap.aldabaknocking.com/code/arpsniffer.c>