International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://dx.doi.org/10.7324/IJASRE.2017.32509 Vol.3 (9) Oct - 2017

Nonconventional Network Security Measures for Intrusion Detection

Sarhan M. Musa, Jaharre Shepard, and Cajetan M. Akujuobi

SECURE Center of Excellence
Prairie View A&M University
Prairie View, TX 77446
USA

ABSTRACT

Cyber-attacks such as Malware, data breaches, denial of service, phishing are proliferating. Network analytic tools such as wire shark and nmap which provide an intelligent about all the bits/frames/packets/data traversing network information are essential for Cyber Security. This paper studies the advantages the packet sniffing as well as the security scanner and the command prompt for the analysis of a network for security purposes. We demonstrate methods that can be taken to detect possible unwanted or foreign devices within the network, despite sniffing software's not truly being designed for security measures.

Keywords: Cyber Security, Traffic analyzer, Network Sniffing, Wi-Fi.

1. INTRODUCTION

Today, there is a need for information security and increase of risk analysis professionals due to industries entities become increasingly dependent on computer technology to transmit and store sensitive data, intellectual property, and financial transactions.

Network intrusion is a serious issue in network security and must be monitored carefully to ensure the network is safe. Network admins must account for the size of the network to estimate the amount of traffic that will be going on daily, and must take the proper measures to monitor the network. With the ever increasing use of technology on all levels, security becomes just as increasingly important. The packet sniffer WireShark and security scanner Nmap, alongside of help from simple commands in the command prompt, can greatly help with network security on many levels.

Admins can use these software's to get an overall list of traffic on the network using WireShark's packet capturing. And with the convenience of being able to sort to see what devices are communicating with what, it can be very effective in smaller let's say home networks. By knowing the IP of the device you would like to track, you can easily sort the capture to see where that device is communicating to and what is communicating to that device.

Nmap works a little more deeper as one of its most common applications is port scanning which will scan a selected IP to see what ports it is using as well as additional information such as if the port is open or closed. Seeing as how many network interiors can enter a network through open ports, this feature can prove quite beneficial.

In this paper, we use network topology as in Figure 1 and running commands from a laptop. Figure 1 shows our network map used to explore these applications. Figure 2 shows a sample of the network used in [2].

From the ISP, the router sends wireless fidelity (Wi-Fi) through the network. All the devices we use are connected wirelessly across the 2.5GHz band. All though connecting via Ethernet is more efficient, we prefer the convenience of Wi-Fi. We also have a few more devices connected to the network, but those are not important.

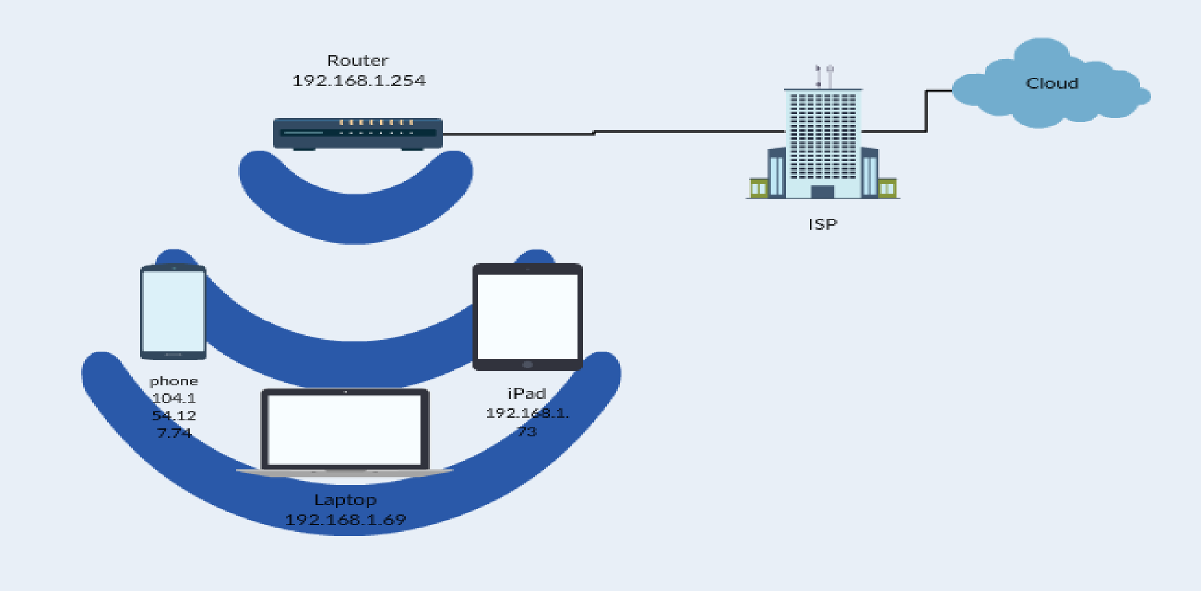


Figure 1.Network topology Map. Map shows all connected TCP devices that connected and communicating with the router during the procedures.

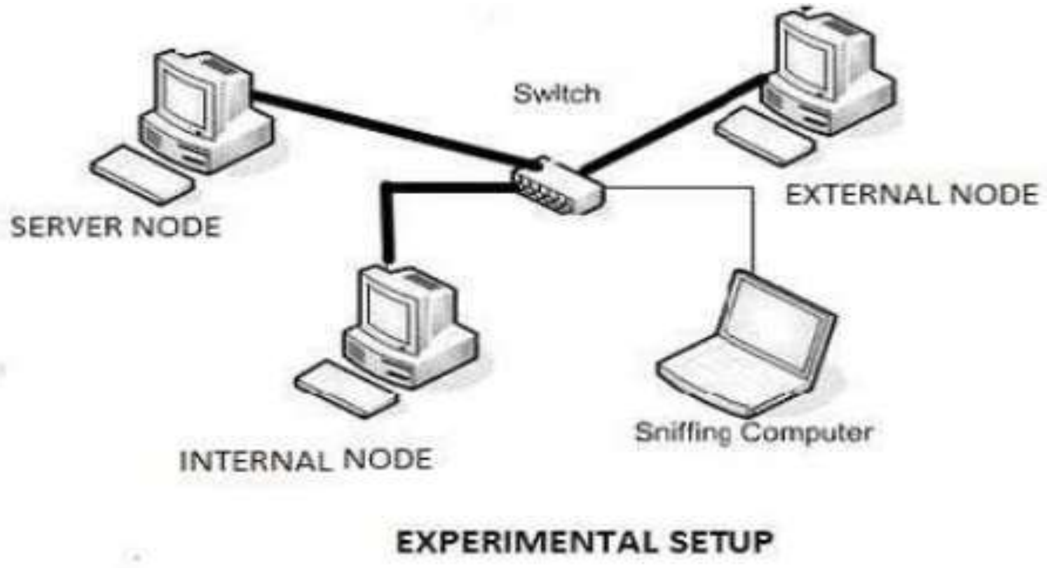


Figure 2.Shows the setup of the sample network [2].

2. NETWORK SECURITY

With technology becoming increasingly more important in today's age with more and more services moving to computers, network security is a very important issue for companies, small businesses, and even home networks [9]. For these large networks, the bandwidth is always important. With the use of IP packet sniffing each device on the network can be seen to determine what is unneeded on the network. The protocols used in these connections will also be available to further determine. There can be extensive amounts of sensitive information that can be available on a PC at any given time. With this in mind system administrators must take extra precaution when monitoring networks. There are many methods and procedures available to help the process. Figure 3 shows the different types of sensitive information that may be contained on a company server due to employee's computer use, as expected the amount of spending is increasing more and more each year.

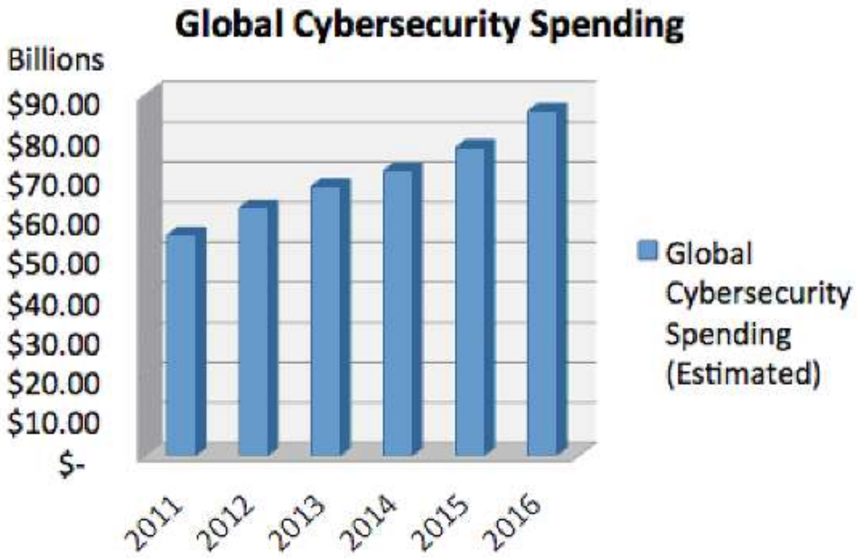


Figure 3.Worldwide spending on cybersecurity [11].

Unfortunately, as technology advances there are thieves and corrupt people in the world who will go to extremes. Just recently in 2016 there were many severe malware attacks at companies.

Figure 4 shows the different type of attacks that happened to companies and users during 2013.

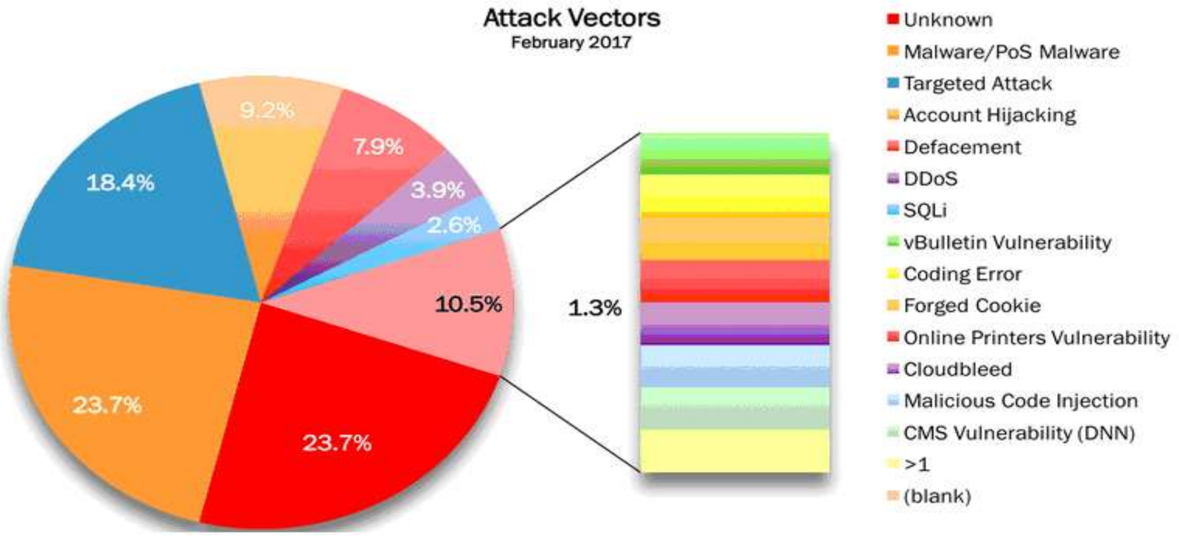


Figure 4. This shows the different type of attacks that happened to companies and users during 2013. DDos makes up a vast majority of attacks done on any network [8].

These attacks left many company networks inaccessible causing them to ultimately lose money due to their networks being down. These hackers would encrypt the networks leaving the companies with messages saying that the malware will not be removed until large payments were made. The tragic thing is that many of these companies were nearly forced to pay these ransoms or risk trying to find their own solution which may take even longer for them to figure out causing them to lose money. These types of situations happen which goes to show the importance of protecting your network to protect your privacy. The large number of DDos attacks are affecting security in organizations that is very hard to recognize and become undetected until the event happens [8].

There are many different methods to ensure that monitoring is done ethically to not intrude on user's privacy. Fifty one percents of employees, who use the internet at work, spend 1 to 5 hours per week surfing the internet for personal reasons [1]. This will greatly increase overall traffic over the network potentially exposing it to more opportunities for intruders. This also feeds into the reason why network monitoring on large networks can be critical in maintaining daily network safety. To monitor, experts use packet sniffing which will detect and interpret all incoming and outgoing traffic on the network [1].

Network Intrusion Detection System or NIDS is an independent system that monitors the network traffic and analyzes them if they are free from attack or not. Network Intrusion Detection System (NIDS) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for malicious activity. Traffic on the network may consist of any connection, Connectionless or connection-oriented. Connectionless use User Datagram Protocol (UDP) and connection-oriented use Transmission control Protocol (TCP) [6]. Wireless Local Area Networks (WLANs) are extremely subject to these types of attacks and it is a huge concern for network admins [9]. Users and admins should also be aware of the threats of the wireless security protocols; wired equivalent privacy WEP, WiFi protected access WPA and Robust Security Network RSN [10].

3. INTRODUCTION TO WIRESHARK PACKET SNIFFER

WireShark is a packet sniffer that works on many different operating systems. It is what is considered to be a passive analyzer, which means it is only able to capture packets and not manipulate them. It can be used as a tool to detect network intrusions, however it is still very useful tool for helping network admins troubleshoot a network. Reference [2] describes a packet sniffer as "its purpose is to monitor network assets to detect anomalous behavior and misuse [2]. A packet sniffer can also be thought of as, an application which can capture and analyze network traffic which is passing through a system's Network Interface Card or NIC [7].

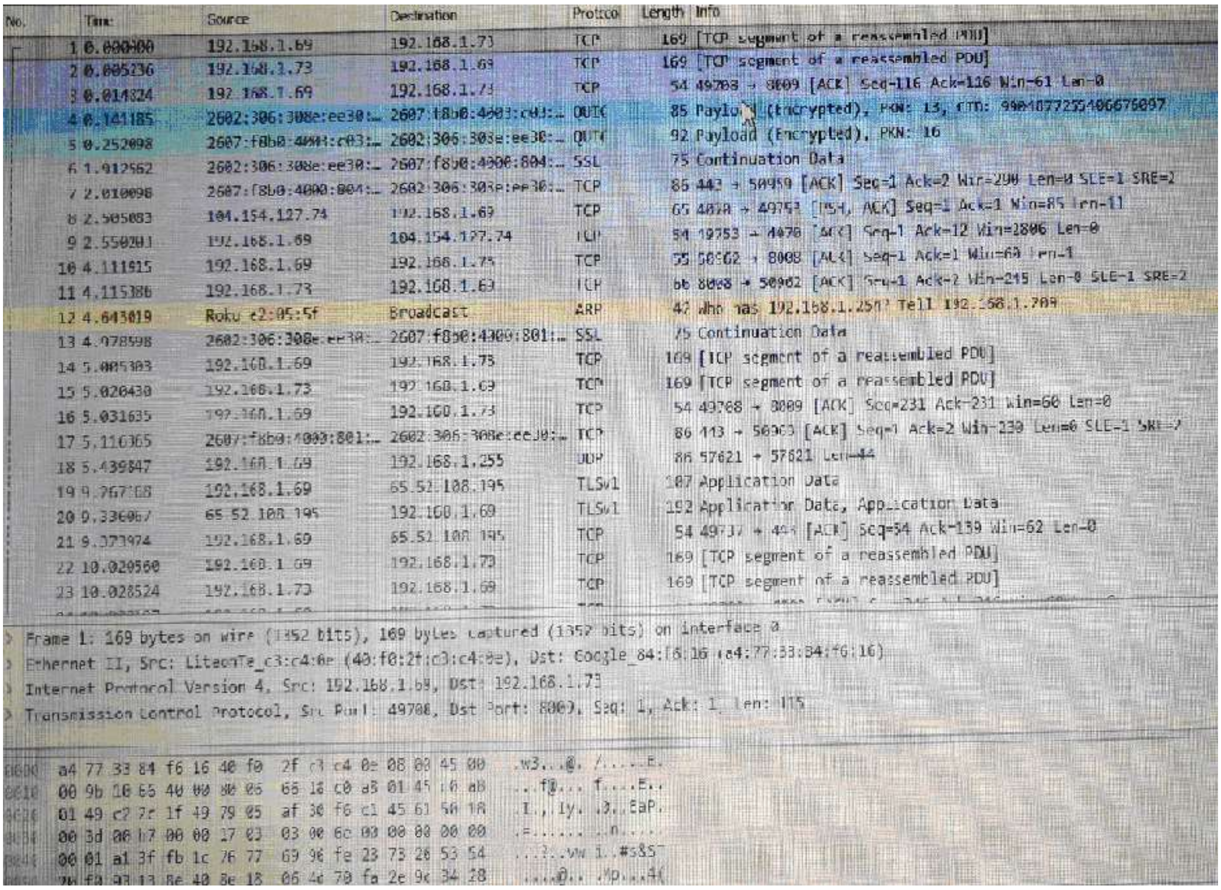
Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998 [5].

A packet sniffer is computer software that runs simultaneously with applications so that a user can interpret, debug, and analyze incoming and outcoming packets. It analyzes the packets by intercepting all network traffic that the software can see or the user allows. Once the network traffic is read the software will take all of its components and present it to the user with details of both ends of the communication. For network administrators, this software is very important as it allows them to easily manage all devices on a large network.

3.1 Security Methods in WireShark

For a user who may think that there network may have been compromised, there are a few methods that are available to try to detect these issues. Firstly, we can start by simply doing a capture of the network to see all active data transfers. Ensure that promiscuous mode is selected which means that all traffic will be read, whether it is an addressed machine or not [7]. Before capturing we should first clear your browser's cache and then select a filter if desired, filtering is only necessary in very large networks, and then press start at the bottom of the Capture Interface to begin the capture process.

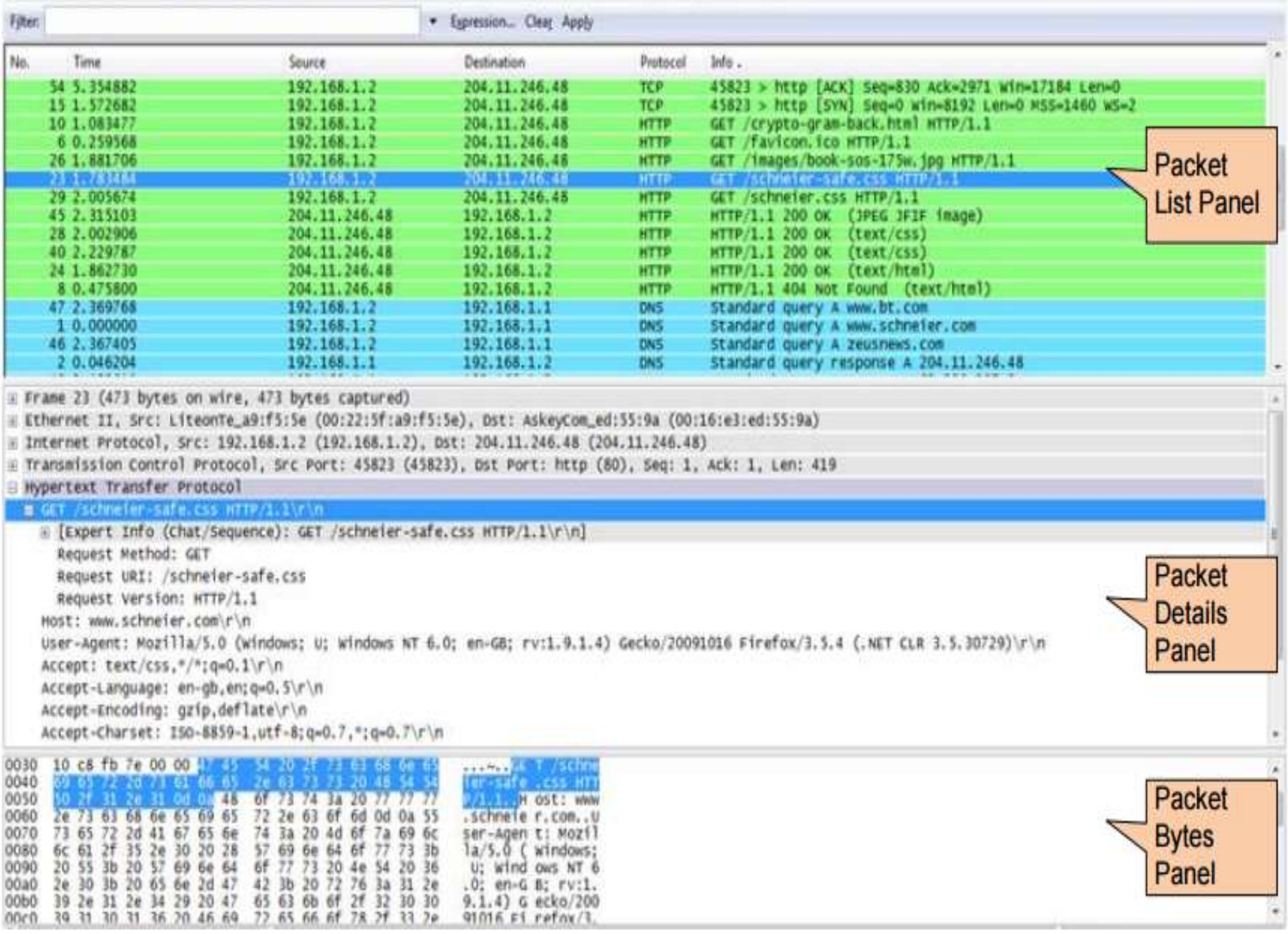
Once we start the capture, a blank window will appear and after a few seconds you will start to see information appear, the capture will continuously record information. After a few seconds you should have something similar to Figure 5, depending on how long you allow the capture to run, the Figure 5 capture was ran for about ten seconds. This screen will show detailed information about the communication between source and destination devices, the time it took to capture the communication, the protocol used, and the length of the packets communicated. As long as a device is powered and connected to the network, it will periodically communicate with the network even if it is only sending small update messages [5].



```
No.  Time         Source                    Destination               Protocol Length Info
  1 0.000000     192.168.1.69              192.168.1.73              TCP      169 [TCP segment of a reassembled PDU]
  2 0.005236     192.168.1.73              192.168.1.69              TCP      169 [TCP segment of a reassembled PDU]
  3 0.014824     192.168.1.69              192.168.1.73              TCP       54 49708 → 8009 [ACK] Seq-116 Ack-116 Win-61 Len-0
  4 0.141185     2602:306:308e:ee30:…      2607:f8b0:4003:c03:…      QUIC      85 Payload (Encrypted), PKN: 13, CID: 9904077255406676097
  5 0.252098     2607:f8b0:4003:c03:…      2602:306:308e:ee30:…      QUIC      92 Payload (Encrypted), PKN: 16
  6 1.912562     2602:306:308e:ee30:…      2607:f8b0:4000:804:…      SSL       75 Continuation Data
  7 2.010096     2607:f8b0:4000:804:…      2602:306:308e:ee30:…      TCP       86 443 → 50959 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
  8 2.505083     104.154.127.74            192.168.1.69              TCP       65 4070 → 49753 [PSH, ACK] Seq=1 Ack=1 Win=85 Len=11
  9 2.550201     192.168.1.69              104.154.127.74            TCP       54 49753 → 4070 [ACK] Seq-1 Ack-12 Win=2806 Len=0
 10 4.111915     192.168.1.69              192.168.1.75              TCP       55 50962 → 8008 [ACK] Seq-1 Ack=1 Win=60 Len-1
 11 4.115386     192.168.1.73              192.168.1.69              TCP       66 8008 → 50962 [ACK] Seq-1 Ack-2 Win-215 Len-0 SLE-1 SRE=2
 12 4.643019     Roku_e2:05:5f             Broadcast                 ARP       42 Who has 192.168.1.250? Tell 192.168.1.709
 13 4.978598     2602:306:308e:ee30:…      2607:f8b0:4000:801:…      SSL       75 Continuation Data
 14 5.005303     192.168.1.69              192.168.1.75              TCP      169 [TCP segment of a reassembled PDU]
 15 5.020430     192.168.1.73              192.168.1.69              TCP      169 [TCP segment of a reassembled PDU]
 16 5.031635     192.168.1.69              192.168.1.73              TCP       54 49768 → 8009 [ACK] Seq=231 Ack-231 Win=60 Len=0
 17 5.116365     2607:f8b0:4000:801:…      2602:306:308e:ee30:…      TCP       86 443 → 50963 [ACK] Seq=1 Ack=2 Win-230 Len=0 SLE-1 SRE=2
 18 5.439847     192.168.1.69              192.168.1.255             UDP       86 57621 → 57621 Len=44
 19 9.267168     192.168.1.69              65.52.108.195             TLSv1    107 Application Data
 20 9.336067     65.52.108.195             192.168.1.69              TLSv1    192 Application Data, Application Data
 21 9.373974     192.168.1.69              65.52.108.195             TCP       54 49737 → 443 [ACK] Seq=54 Ack-139 Win=62 Len-0
 22 10.020560    192.168.1.69              192.168.1.73              TCP      169 [TCP segment of a reassembled PDU]
 23 10.028524    192.168.1.73              192.168.1.69              TCP      169 [TCP segment of a reassembled PDU]

> Frame 1: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface 0
> Ethernet II, Src: LiteonTe_c3:c4:8e (40:f0:2f:c3:c4:8e), Dst: Google_84:f6:16 (a4:77:33:84:f6:16)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 192.168.1.73
> Transmission Control Protocol, Src Port: 49708, Dst Port: 8009, Seq: 1, Ack: 1, Len: 115

0000  a4 77 33 84 f6 16 40 f0  2f c3 c4 8e 08 00 45 00   .w3...@. /.....E.
0010  00 9b 10 65 40 00 80 06  66 16 c0 a8 01 45 c0 a8   ...e@... f....E..
0020  01 49 c2 2c 1f 49 79 05  af 30 f6 c1 45 61 50 18   .I.,.Iy. .0..EaP.
0030  00 3d 00 b7 00 00 17 03  03 00 6c 00 00 00 00 00   .=...... ..l.....
0040  00 01 a1 3f fb 1c 76 77  69 96 fe 23 73 26 53 54   ...?..vw i..#s&ST
0050  7e f0 93 13 8e 40 8e 18  06 4c 70 fa 2e 9c 34 28   ~....@.. .Lp...4(
```

Figure 5. Sample capture taken of the tested network. In this capture you can see all devices shown in the network diagram.

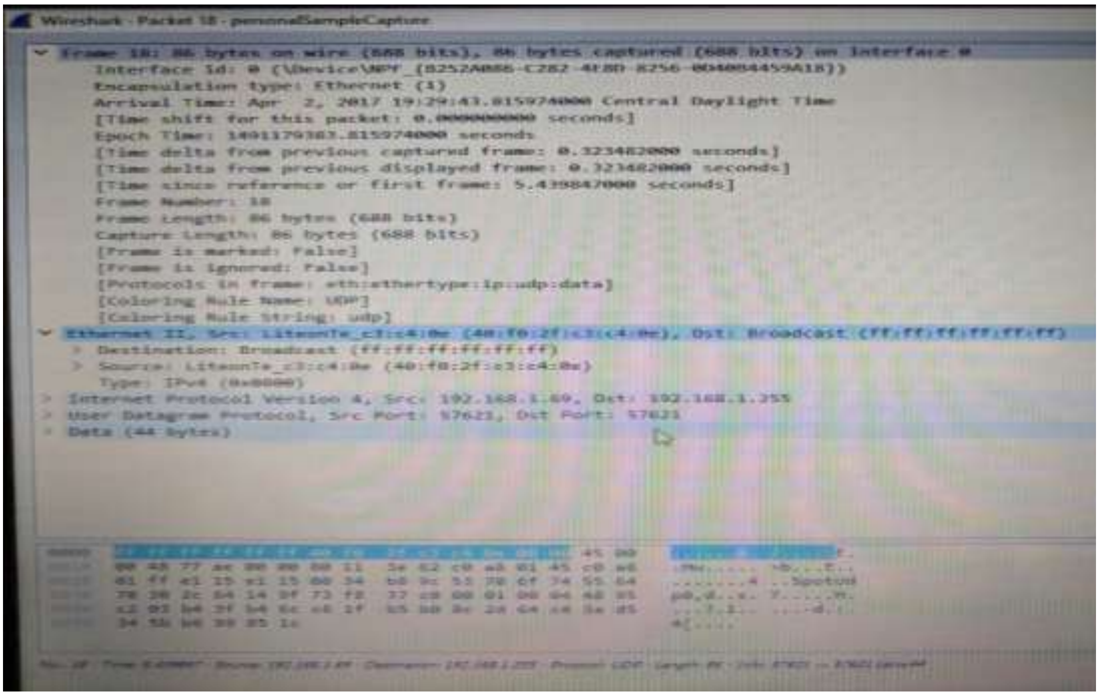
The capture will have three separate columns of information as in Figure 6. The packet list panel will list the packets in the current capture. The packet details panel shows details of the selected packet. It shows the different TCP/UDP/ISMP, and application protocols as well. The packet bytes panel will show bytes in hexadecimal and ASCII encodings [7]. As predicted I received a similar capture to the sample. The capture will vary depending on the size of the network.



```
No.  Time       Source          Destination     Protocol  Info .
 54 5.354882    192.168.1.2     204.11.246.48   TCP       45823 > http [ACK] Seq=830 Ack=2971 Win=17184 Len=0
 15 1.572682    192.168.1.2     204.11.246.48   TCP       45823 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
 10 1.083477    192.168.1.2     204.11.246.48   HTTP      GET /crypto-gram-back.html HTTP/1.1
  6 0.259568    192.168.1.2     204.11.246.48   HTTP      GET /favicon.ico HTTP/1.1
 26 1.881706    192.168.1.2     204.11.246.48   HTTP      GET /images/book-sos-175w.jpg HTTP/1.1
 23 1.783484    192.168.1.2     204.11.246.48   HTTP      GET /schneier-safe.css HTTP/1.1
 29 2.005674    192.168.1.2     204.11.246.48   HTTP      GET /schneier.css HTTP/1.1
 45 2.315103    204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (JPEG JFIF image)
 28 2.002906    204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/css)
 40 2.229787    204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/css)
 24 1.862730    204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 200 OK  (text/html)
  8 0.475800    204.11.246.48   192.168.1.2     HTTP      HTTP/1.1 404 Not Found  (text/html)
 47 2.369768    192.168.1.2     192.168.1.1     DNS       Standard query A www.bt.com
  1 0.000000    192.168.1.2     192.168.1.1     DNS       Standard query A www.schneier.com
 46 2.367405    192.168.1.2     192.168.1.1     DNS       Standard query A zeusnews.com
  2 0.046204    192.168.1.1     192.168.1.2     DNS       Standard query response A 204.11.246.48

⊞ Frame 23 (473 bytes on wire, 473 bytes captured)
⊞ Ethernet II, Src: LiteonTe_a9:f5:5e (00:22:5f:a9:f5:5e), Dst: AskeyCom_ed:55:9a (00:16:e3:ed:55:9a)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 204.11.246.48 (204.11.246.48)
⊞ Transmission Control Protocol, Src Port: 45823 (45823), Dst Port: http (80), Seq: 1, Ack: 1, Len: 419
⊟ Hypertext Transfer Protocol
  ■ GET /schneier-safe.css HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /schneier-safe.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /schneier-safe.css
      Request Version: HTTP/1.1
    Host: www.schneier.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-GB; rv:1.9.1.4) Gecko/20091016 Firefox/3.5.4 (.NET CLR 3.5.30729)\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: en-gb,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n

0030  10 c8 fb 7e 00 00 47 45  54 20 2f 73 63 68 6e 65   ...~..GE T /schne
0040  69 65 72 2d 73 61 66 65  2e 63 73 73 20 48 54 54   ier-safe .css HTT
0050  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77   P/1.1..H ost: www
0060  2e 73 63 68 6e 65 69 65  72 2e 63 6f 6d 0d 0a 55   .schneie r.com..U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0080  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 3b   la/5.0 ( Windows;
0090  20 55 3b 20 57 69 6e 64  6f 77 73 20 4e 54 20 36    U; Wind ows NT 6
00a0  2e 30 3b 20 65 6e 2d 47  42 3b 20 72 76 3a 31 2e   .0; en-G B; rv:1.
00b0  39 2e 31 2e 34 29 20 47  65 63 6b 6f 2f 32 30 30   9.1.4) G ecko/200
00c0  39 31 30 31 36 20 46 69  72 65 66 6f 78 2f 33 2e   91016 Fi refox/3.
```

Figure 6. Sample captured using the same techniques.

Figure 7 shows when we double click on the frame, it will bring up additional information about the particular frame.



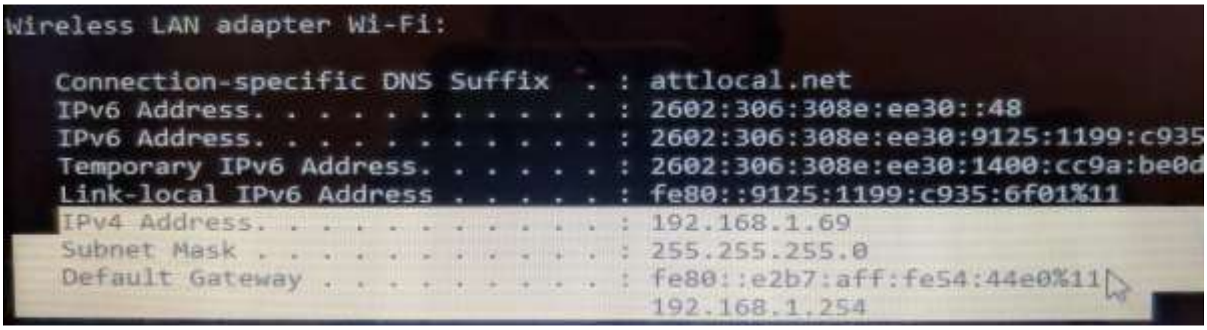
```
˅ Frame 18: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
    Interface id: 0 (\Device\NPF_{8252A086-C282-4F8D-8256-0040B4459A18})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr  2, 2017 19:29:43.815974000 Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1491179383.815974000 seconds
    [Time delta from previous captured frame: 0.323482000 seconds]
    [Time delta from previous displayed frame: 0.323482000 seconds]
    [Time since reference or first frame: 5.439847000 seconds]
    Frame Number: 18
    Frame Length: 86 bytes (688 bits)
    Capture Length: 86 bytes (688 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
˅ Ethernet II, Src: LiteonTe_c3:c4:0e (40:f0:2f:c3:c4:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: LiteonTe_c3:c4:0e (40:f0:2f:c3:c4:0e)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 192.168.1.255
> User Datagram Protocol, Src Port: 57621, Dst Port: 57621
> Data (44 bytes)
```

[illegible]

Figure 7. Double clicking on a frame will bring up additional information about the particular frame.Depending on the size of your network this method can prove useful to detecting foreign and unknown devices on your network. With the capture screen opened, you can select how the captured information is displayed by number, time, source IP, destination IP, protocol, and length. For this application I would suggest using either the source or destination IP, but this will make no difference in the result just for

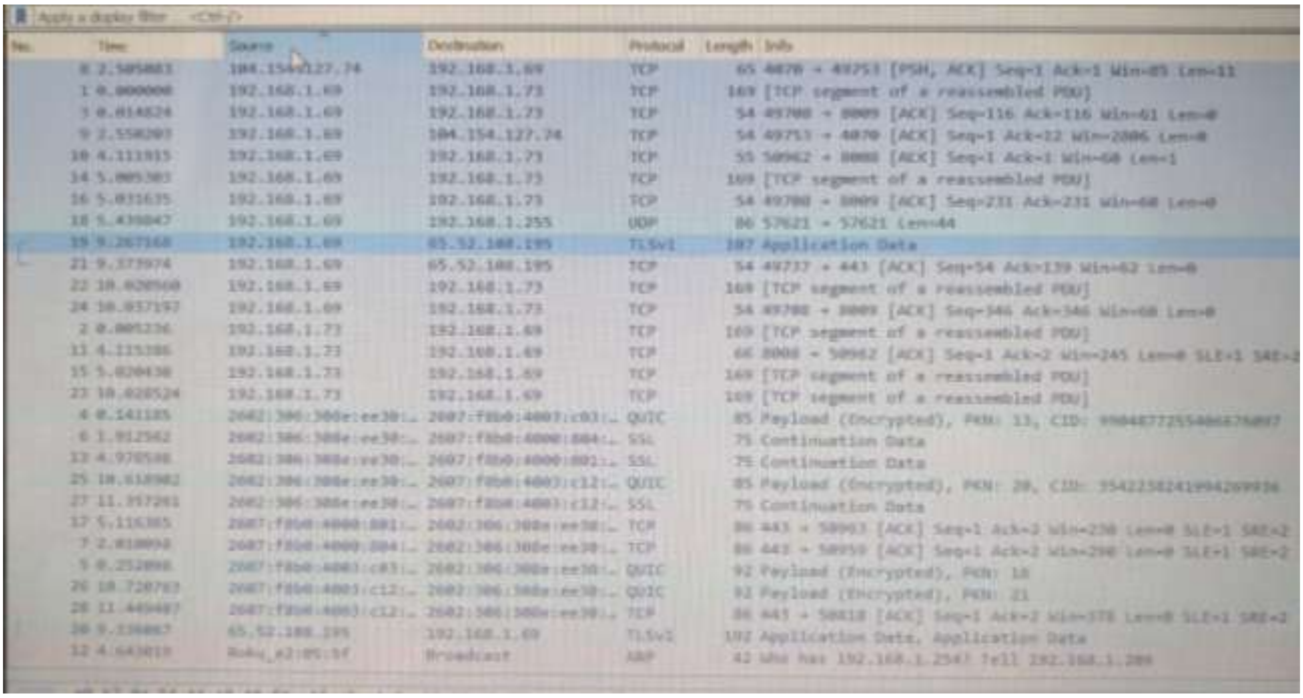
clarity while reading results. Reference [1] explains the filtering available to look at only certain types of packets such as TCP etc. Depending on the size of the network, it may be beneficial to filter before taking the capture depending on what the user is looking for.

Figure 8 shows the network sorted by sources to their various destinations. By entering ‘ipconfig’ into the command prompt I was able to find the IP address of the laptop; which is 192.168.1.69. The ipconfig command will also show the router IP; which will be listed under the default gateway, mine is 192.168.1.254. The WireShark capture and ipconfig command were not taken at the sametime, which is why the router IP in the Wireshark capture is 192.168.1.255. The theWireShark capture can be referred to in Figure 9 for the capture sorted by Source. This allows us to see what particular source IP is communicating to corresponding destination IPs.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : attlocal.net
   IPv6 Address. . . . . . . . . . . : 2602:306:308e:ee30::48
   IPv6 Address. . . . . . . . . . . : 2602:306:308e:ee30:9125:1199:c935
   Temporary IPv6 Address. . . . . . : 2602:306:308e:ee30:1400:cc9a:be0d
   Link-local IPv6 Address . . . . . : fe80::9125:1199:c935:6f01%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.69
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::e2b7:aff:fe54:44e0%11
                                       192.168.1.254
```

Figure 8.Snapshot of the result of the ipconfig command in the user prompt. The default gateway value will be the IP for the router.



```
Apply a display filter ... <Ctrl-/>
No.  Time        Source                Destination           Protocol Length Info
  8  2.505883    104.154.127.74        192.168.1.69          TCP        65 4070 → 49753 [PSH, ACK] Seq=1 Ack=1 Win=85 Len=11
  1  0.000000    192.168.1.69          192.168.1.73          TCP       169 [TCP segment of a reassembled PDU]
  3  0.014824    192.168.1.69          192.168.1.73          TCP        54 49708 → 8009 [ACK] Seq=116 Ack=116 Win=61 Len=0
  9  2.550207    192.168.1.69          104.154.127.74        TCP        54 49753 → 4070 [ACK] Seq=1 Ack=12 Win=2006 Len=0
 10  4.111915    192.168.1.69          192.168.1.73          TCP        55 50962 → 8008 [ACK] Seq=1 Ack=1 Win=60 Len=1
 14  5.005303    192.168.1.69          192.168.1.73          TCP       169 [TCP segment of a reassembled PDU]
 16  5.031635    192.168.1.69          192.168.1.73          TCP        54 49708 → 8009 [ACK] Seq=231 Ack=231 Win=60 Len=0
 18  5.430047    192.168.1.69          192.168.1.255         UDP        86 57621 → 57621 Len=44
 19  9.267168    192.168.1.69          65.52.108.195         TLSv1     107 Application Data
 21  9.373974    192.168.1.69          65.52.108.195         TCP        54 49737 → 443 [ACK] Seq=54 Ack=139 Win=62 Len=0
 22  10.020560   192.168.1.69          192.168.1.73          TCP       169 [TCP segment of a reassembled PDU]
 24  10.037197   192.168.1.69          192.168.1.73          TCP        54 49708 → 8009 [ACK] Seq=346 Ack=346 Win=60 Len=0
  2  0.005236    192.168.1.73          192.168.1.69          TCP       169 [TCP segment of a reassembled PDU]
 11  4.115386    192.168.1.73          192.168.1.69          TCP        66 8008 → 50962 [ACK] Seq=1 Ack=2 Win=245 Len=0 SLE=1 SRE=2
 15  5.020430    192.168.1.73          192.168.1.69          TCP       169 [TCP segment of a reassembled PDU]
 23  10.028524   192.168.1.73          192.168.1.69          TCP       169 [TCP segment of a reassembled PDU]
  4  0.141185    2602:306:308e:ee30:…  2607:f8b0:4007:c03:…  QUIC       85 Payload (Encrypted), PKN: 13, CID: 9904877255406876097
  6  1.912562    2602:306:308e:ee30:…  2607:f8b0:4000:804:…  SSL        75 Continuation Data
 13  4.970508    2602:306:308e:ee30:…  2607:f8b0:4000:801:…  SSL        75 Continuation Data
 25  10.618982   2602:306:308e:ee30:…  2607:f8b0:4003:c12:…  QUIC       85 Payload (Encrypted), PKN: 20, CID: 3542258241994269936
 27  11.357201   2602:306:308e:ee30:…  2607:f8b0:4003:c12:…  SSL        75 Continuation Data
 17  5.116365    2607:f8b0:4000:801:…  2602:306:308e:ee30:…  TCP        86 443 → 50963 [ACK] Seq=1 Ack=2 Win=230 Len=0 SLE=1 SRE=2
  7  2.010094    2607:f8b0:4000:804:…  2602:306:308e:ee30:…  TCP        86 443 → 50959 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
  5  0.252098    2607:f8b0:4003:c03:…  2602:306:308e:ee30:…  QUIC       92 Payload (Encrypted), PKN: 18
 26  10.720763   2607:f8b0:4003:c12:…  2602:306:308e:ee30:…  QUIC       92 Payload (Encrypted), PKN: 21
 28  11.449487   2607:f8b0:4003:c12:…  2602:306:308e:ee30:…  TCP        86 443 → 50818 [ACK] Seq=1 Ack=2 Win=378 Len=0 SLE=1 SRE=2
 30  9.330067    65.52.108.195         192.168.1.69          TLSv1     192 Application Data, Application Data
 12  4.643019    Roku_a2:05:5f         Broadcast             ARP        42 Who has 192.168.1.254? Tell 192.168.1.200
```

Figure 9. Capture sorted by Source.

3.2 Implementing Actions

With the information gained from the WireShark you can begin to take action on the network if intrusion is suspected. For example, if you have a small home network with only a few devices it would easy to detect foreign devices within the network. With the key information gained from the ipconfig command, we now know the IP of the router which means you could go to the capture and sort the capture by destination to focus on devices sending packets to the router.

Based on the results further action may need to be taken. We may need to go through all of the devices and find IPs for them to see their activity on the network. Also, we may find that there are a few weird sources and destinations that appear under odd protocols.

If intrusion is detected there are a couple things you can do to help secure the network. Firstly, we want to always make sure all aspects of your network are protected with a password. This can keep the neighbor or anyone near by from easily connecting to the network and taking up the bandwidth. If suspicious activity is suspected and we do have a password on the router we may need to take more advanced steps. By going into the router's advanced settings, it is possible to see client names of the devices connected to the network where foreign devices can also be kicked from the network [5].

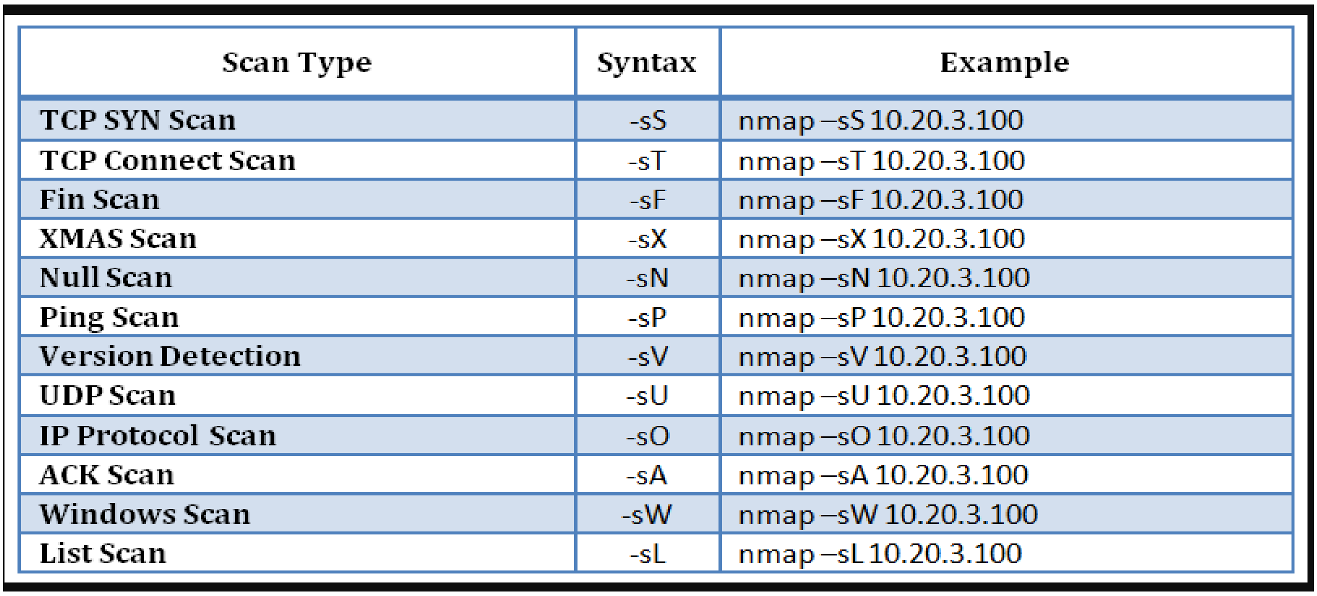
These steps will work fine for a small network, but what about for a network with many devices connected. For these size of networks there are softwares out there specifically designed to alert the admin when unwanted devices are connected. Snort is a very popular and free IDS (intrusion detection software) that is widely used. The user can set the guidelines of snort to tell up what is acceptable and not acceptable IPs on the network. For example as an admin I have the ability to set the IP of devices on the network. I may only want my computers to have IPs of 191.168.1.xxx and for all other devices with different IPs I may want snort to alert me if they are detected. This will allow an admin to quickly take action to remove these unwanted devices.

3.3 Nmap Software

Nmapis popular free networking software that works as a security scanner to discover hosts and services on a computer network, which will build a map of the network. Nmap does this by sending specially crafted packets to the target hosts and will then analyze the response. The software provides a number of features for probing computer networks, including host discovery and service and operating-system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan [4]. Table 1 illustrates a list of basic fundamental commands executable in the command prompt; which corresponds for Nmap.

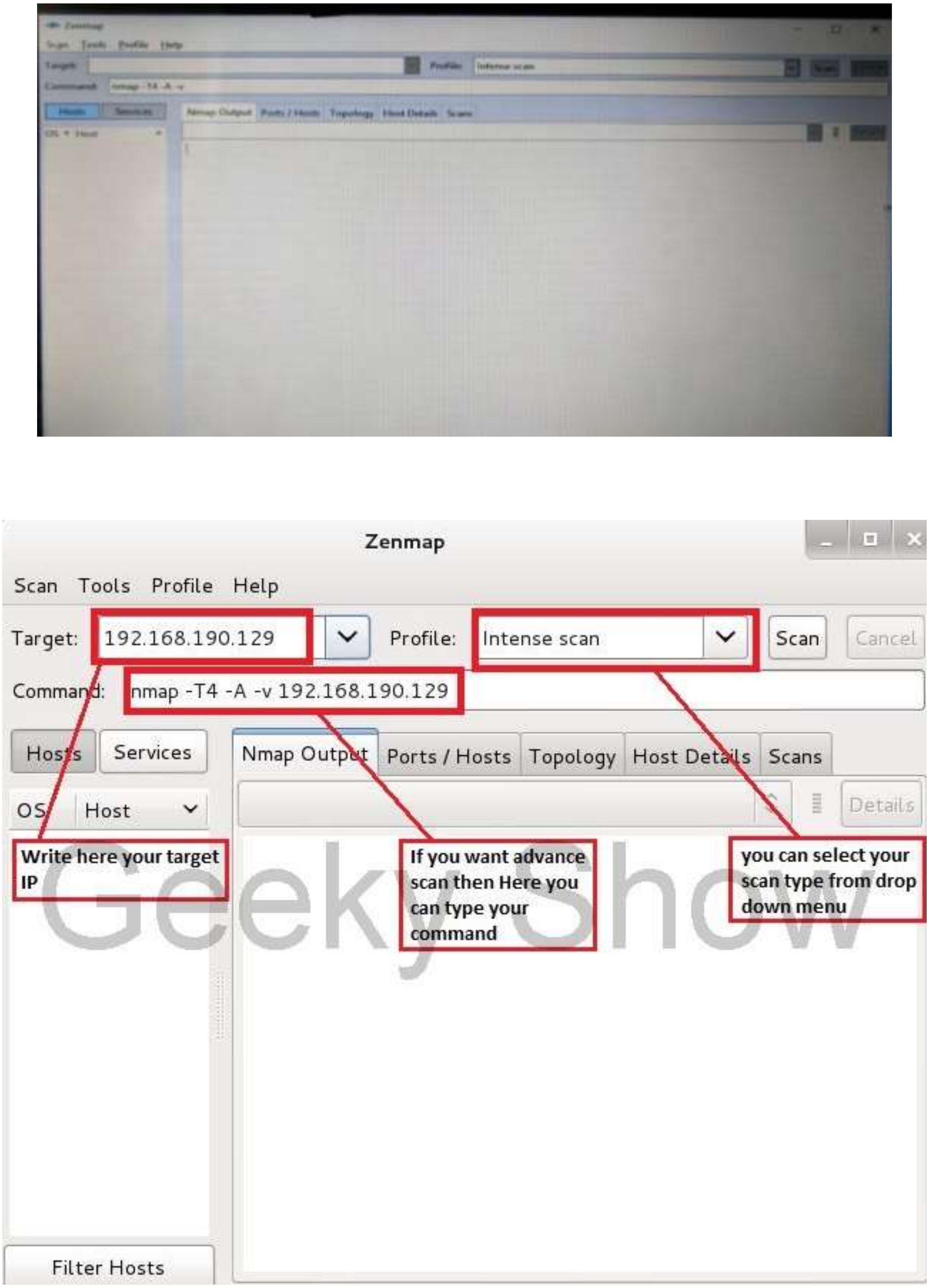
A host scan is typically done over an entire network and will report all machines that are alive on the network. A port scan can be performed on a single, remote, host system, via its IP address and will give information on services running on the machine. Typically attackers are looking for the OS system, TCP and UDP ports that can be exploited. The information that Nmap sends back to the user will show these open ports allowing for an attacker to intrude on the network.

Table 1: List of basic fundamental commands executable in the command prompt for Nmap



Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap –sS 10.20.3.100
TCP Connect Scan	-sT	nmap –sT 10.20.3.100
Fin Scan	-sF	nmap –sF 10.20.3.100
XMAS Scan	-sX	nmap –sX 10.20.3.100
Null Scan	-sN	nmap –sN 10.20.3.100
Ping Scan	-sP	nmap –sP 10.20.3.100
Version Detection	-sV	nmap –sV 10.20.3.100
UDP Scan	-sU	nmap –sU 10.20.3.100
IP Protocol Scan	-sO	nmap –sO 10.20.3.100
ACK Scan	-sA	nmap –sA 10.20.3.100
Windows Scan	-sW	nmap –sW 10.20.3.100
List Scan	-sL	nmap –sL 10.20.3.100

Figure 10 shows the opening screen of Nmap version 7.40 for the first figure. From here we can enter commands needed and targets that need to be observed. The second version shows a detailed layout of the features directly available from the start up screen.



Target: 192.168.190.129

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.190.129

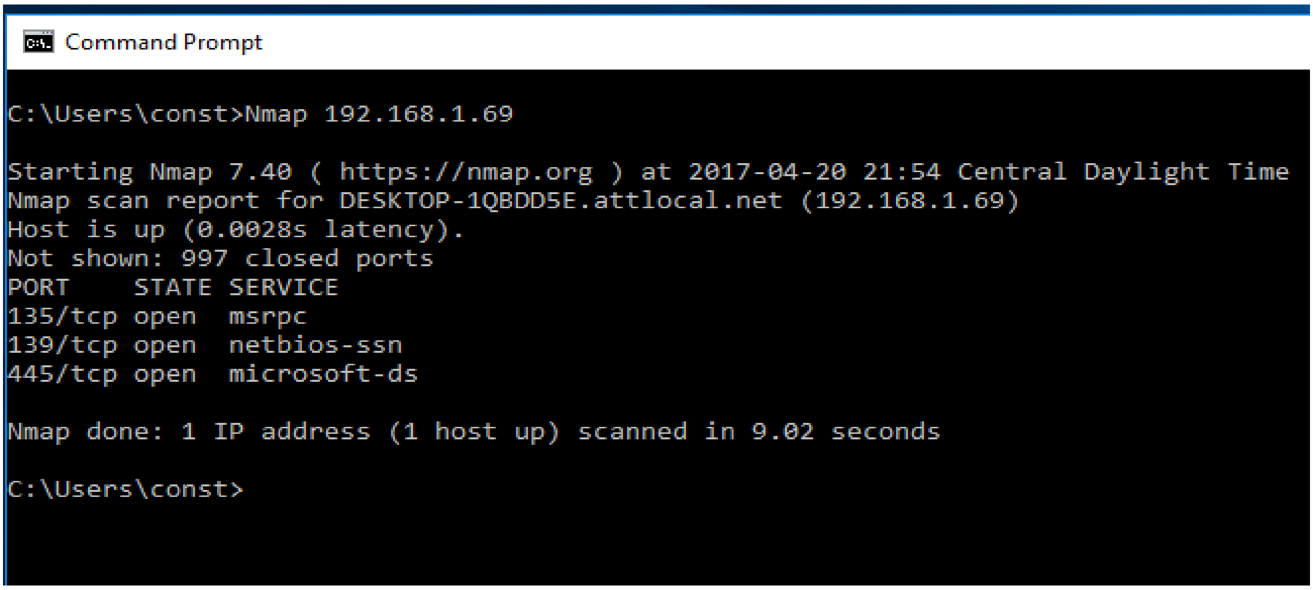
Write here your target IP

If you want advance scan then Here you can type your command

you can select your scan type from drop down menu

Figure 10.The opening screen of Nmap version 7.40 for the first figure.

Most work using Nmap are recommended to be done in the command such as target scanning and host scanning. Target scanning can be completed by simply using this command in the command prompt ‘nampxxx.xxx.x.xx’. This scan will show the status of different ports detected. This information will appear in three columns which are the port scanned and its protocol, the state of the port either open or closed and they service type. Figure 11 shows a host scan of the laptop and the ports that showed up. Three TCP ports are opened and being used.

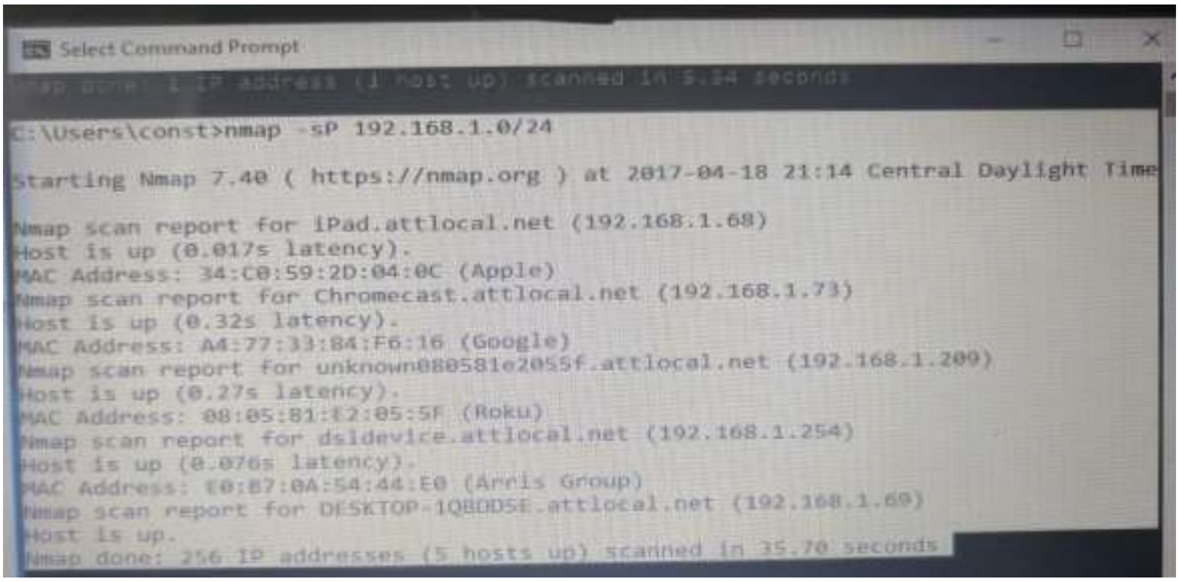


```
C:\Users\const>Nmap 192.168.1.69

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-20 21:54 Central Daylight Time
Nmap scan report for DESKTOP-1QBDD5E.attlocal.net (192.168.1.69)
Host is up (0.0028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 9.02 seconds

C:\Users\const>
```

Figure 11. Result of target scan using laptop IP.

Host scanning is a very powerful command as it will show all active hosts on the network that are on. If the device has not been active, you may have to run a few different scans to capture all devices. With the command prompt open you can enter the command nmap -sPxxx.xxx.x.x, with the x's representing the IP we would like to scan for hosts.

Figure 12 shows the host scan result of my router's IP, 192.168.1.0/24. These methods are listed in reference [4] which is a user guide on doing basic commands using Nmap in the GUI Zenmap and command prompt. Both are equally effective and can be used to obtain the same scan. Host scanning can greatly prevent DDos attacks as open ports are where most intruders enter networks.



```
map done: 1 IP address (1 host up) scanned in 5.34 seconds

C:\Users\const>nmap -sP 192.168.1.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-18 21:14 Central Daylight Time

Nmap scan report for iPad.attlocal.net (192.168.1.68)
Host is up (0.017s latency).
MAC Address: 34:C0:59:2D:04:0C (Apple)
Nmap scan report for Chromecast.attlocal.net (192.168.1.73)
Host is up (0.32s latency).
MAC Address: A4:77:33:84:F6:16 (Google)
Nmap scan report for unknown080581e2055f.attlocal.net (192.168.1.209)
Host is up (0.27s latency).
MAC Address: 08:05:81:E2:05:5F (Roku)
Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.076s latency).
MAC Address: E0:87:0A:54:44:E0 (Arris Group)
Nmap scan report for DESKTOP-1QBDD5E.attlocal.net (192.168.1.69)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 35.70 seconds
```

Figure 12.Host scan of network using command prompt.

4. CONCLUSION

Wire shark and nmap softwares are widely used and can prove to be quite useful by admins in any size network. They both have plenty of methods that can help to decipher larger networks as well as smaller simpler networks. However, with there being so many different types of security breaches going on these days it is always good to have as many measures available to aid in security. In the sense of detecting intrusion already on the network, these methods can prove quite effective for that application. Knowing the makeup and needs of the network should always tell the admin what measures should be taken to ensure safety. Without the proper safety measure, valuable information can be stolen or blocked by intruders leaving the company with some type of ransom or encrypted data. But, with proper networking security methods that can be prevented by all means. Our work demonstrates the advantages the packet sniffing as well as the security scanner and the command prompt for the analysis of a network for security purposes. We introduce methods that can be taken to detect possible unwanted or foreign devices within the network, despite sniffing software's not truly being designed for security measures.

REFERENCES

1. Ben-Eid, Nedhal A. "Ethical Network Monitoring Using WireShark and Colasoft as Sniffing Tools." *International Journal of Advanced Research in Computer and Communication Engineering* 4.3 (2015): 471-78.

2. Banerjee, Usha, AshutoshVashishtha, and MukulSaxena. "Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection ."*International Journal of Computer Applications* (2010): 1-5. Print.

3. https://secur1tyadvisory.wordpress.com/2015/08/29/nmap-for-vulnerability-discovery/

4. http://www.geekyshows.com/2013/07/how-to-use-zenmap-in-kali-linux.html

5. https://www.wireshark.org/#learnWS

6. https://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf

7. Macfarlane, Rich. "Lab 5: Packet Capture & Traffic Analysis with Wireshark." 1-16. Print

8. Avasthi, Deepali. "Network Forensic Analysis with Efficient Preservation for SYN Attack ."*International Journal of Computer Applications* (May 2012): 17-22. Print.

9. El-Nazeer, Nazar, Daimi, Kevin. "Evaluation of Network Port Scanning Tools." Print.

10. H. I. Bulbul, I. Batmaz, and M. Ozel, Wireless network security: comparison of WEP mechanism, WPA and RSN security protocols," *in Proc 1st international conference of Forensic applications and techniques in telecommunications, information, and multimedia, Adelaide, Australia* (January 2008): Print.
11. Ahmed, Humair. "Security, Art of HAcking, & the Worst Security Breaches." <https://www.linkedin.com/pulse/security-art-hacking-worst-2014-breaches-humair-ahmed>, (March 2015)