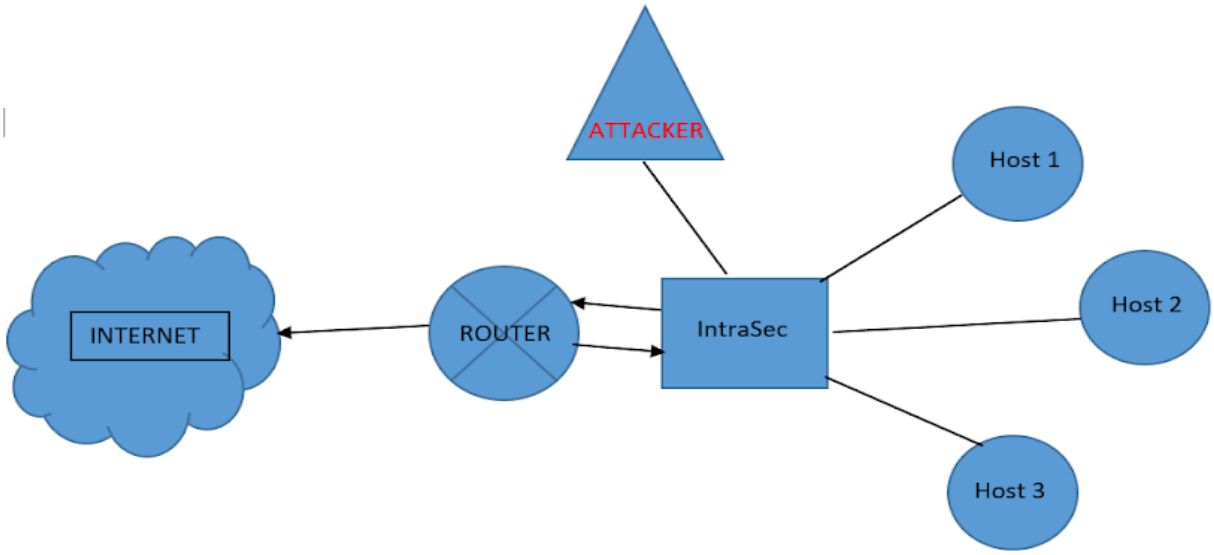
IntraSec – A Black Hat Identification Policy

A. Team Members:

1. Laveen Vasnani (104823402)
2. Pravina Bhatt (104701991)
3. Yixian Hao (104718810)

B. Previous approach overview :

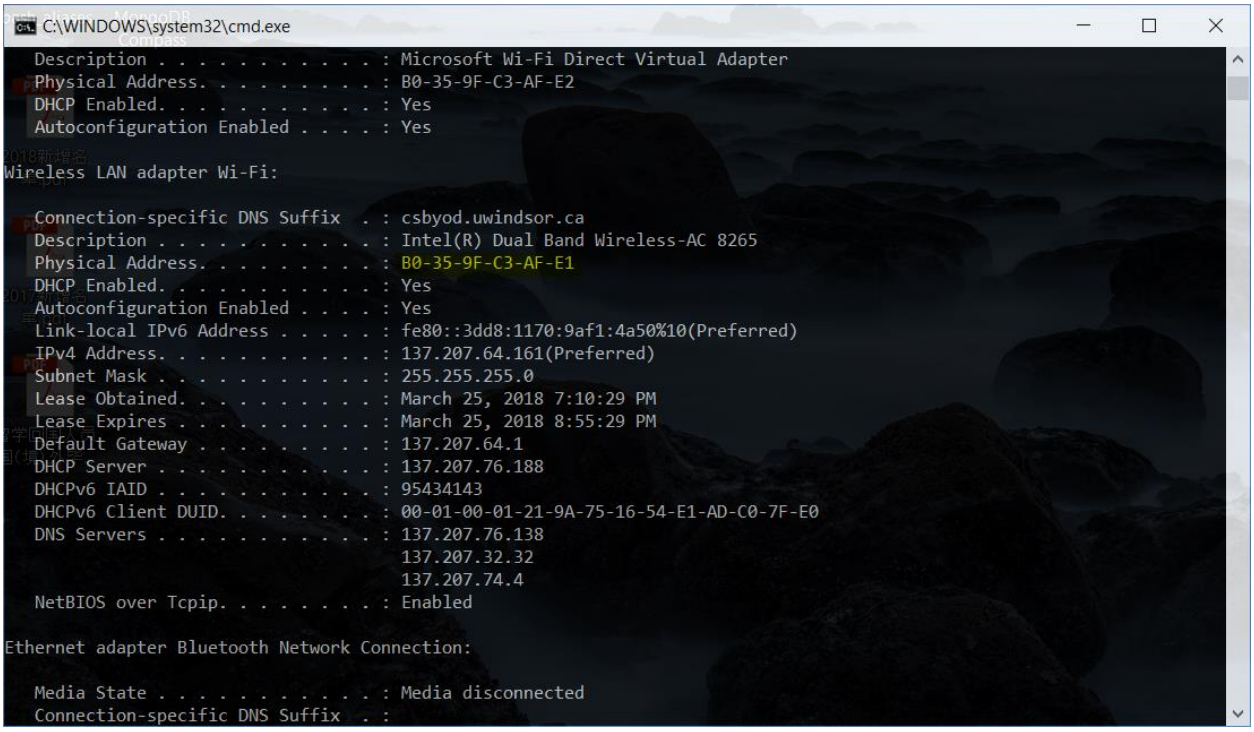


Network sniffer- Who listen to the network and acts as a firewall for the router. Role is divided into two sections as Analyzing and Real Time packet receiving. Real-time part is responsible for receiving the packets from hosts of network including attacker and forward it to later section of detector that is analyzer. Here, Analyzer will be responsible for analyzing incoming packets, compare its details with previously traced ARP table and trace for suspect of some malicious activities performed by any hosts of network.

C. Network Tracing:

- Managing our machine to behave as an Access Point for the current network
- Tracing of packets for every nodes in the network on the basis of declared constraints using python socket programming
- Analysing the packets
- Following screenshots demonstrates network tracing

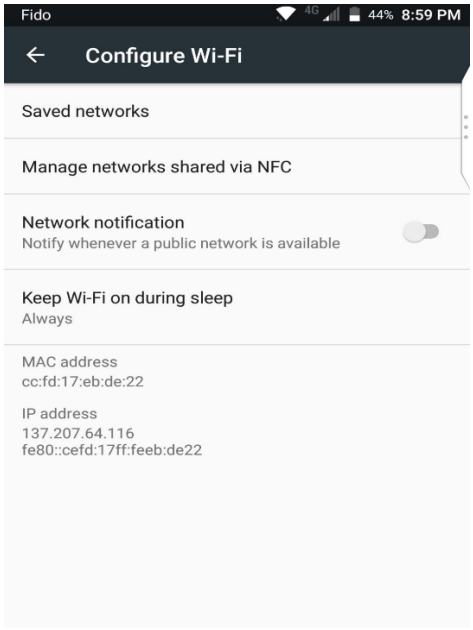
NODE #1:



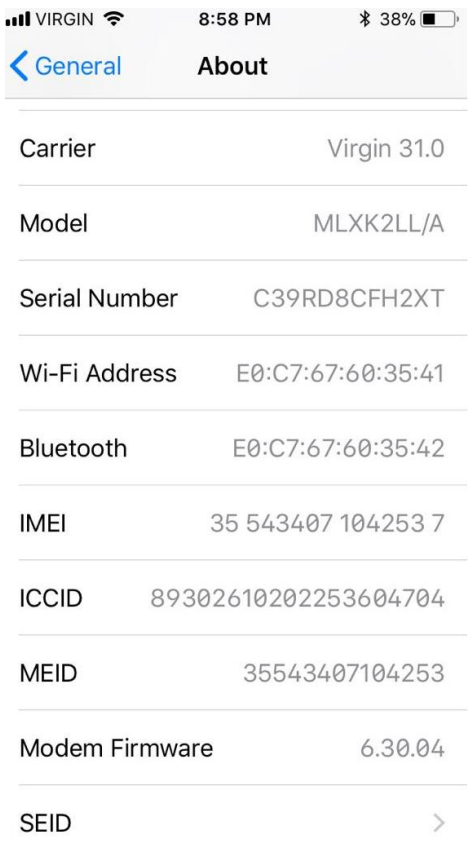
NODE #2:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . : 00-E1-8C-DB-D0-49
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d5e5:9e8d:f603:5199%16(Preferred)
   IPv4 Address. . . . . : 10.241.114.51(Preferred)
   Subnet Mask . . . . . : 255.255.240.0
   Lease Obtained. . . . . : March 25, 2018 5:11:47 PM
   Lease Expires . . . . . : March 25, 2018 7:42:17 PM
   Default Gateway . . . . . : 10.241.112.1
   DHCP Server . . . . . : 137.207.238.52
   DHCPv6 IAID . . . . . : 67166604
   DHCPv6 Client DUID. . . . . : 00-01-00-01-22-0C-33-84-00-E1-8C-DB-D0-49
   DNS Servers . . . . . : 137.207.32.2
                           137.207.32.32
   NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . : Microsoft Teredo Tunneling Adapter
   Physical Address. . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

NODE #3:


Fido
44% 8:59 PM
Configure Wi-Fi
Saved networks
Manage networks shared via NFC
Network notification
Notify whenever a public network is available
Keep Wi-Fi on during sleep
Always
MAC address
cc:fd:17:eb:de:22
IP address
137.207.64.116
fe80::cefd:17ff:feeb:de22

NODE #4:


VIRGIN
8:58 PM
38%
General
About
Carrier
Virgin 31.0
Model
MLXK2LL/A
Serial Number
C39RD8CFH2XT
Wi-Fi Address
E0:C7:67:60:35:41
Bluetooth
E0:C7:67:60:35:42
IMEI
35 543407 104253 7
ICCID
89302610202253604704
MEID
35543407104253
Modem Firmware
6.30.04
SEID

DETECTED NODE # 1

```
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 88:9f:fa:5c:b2:b2 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 88:9f:fa:5c:b2:b2 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : b0:35:9f:c3:af:e1 Protocol : 8
```

DETECTED NODE # 2

```
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 00:c2:c6:4e:16:05 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:16 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:16 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:16 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:16 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:16 Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 88:9f:fa:5c:b2:b2 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 00:e1:8c:db:d0:49 Protocol : 8
```

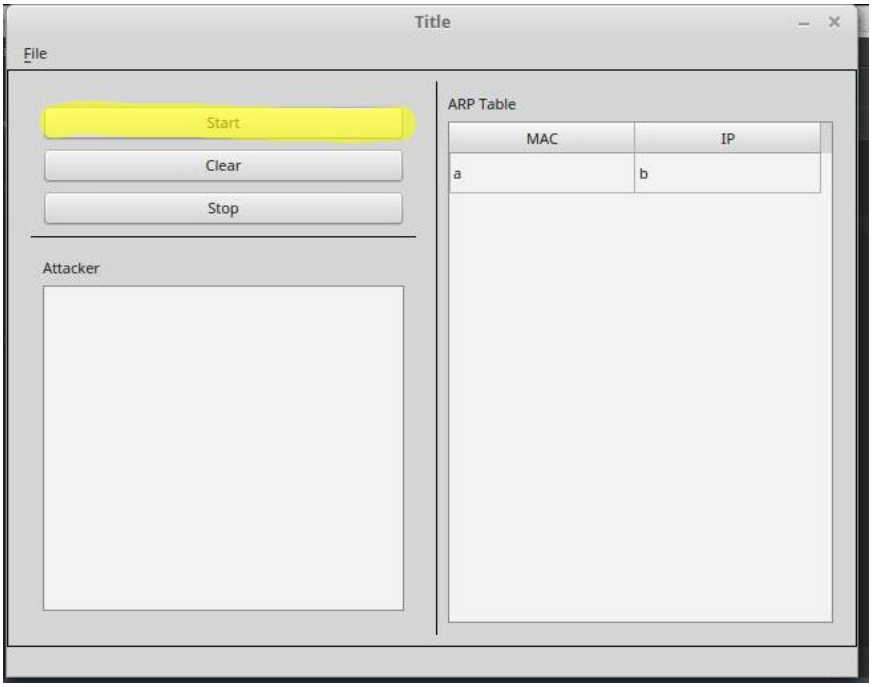
DETECTED NODE # 3

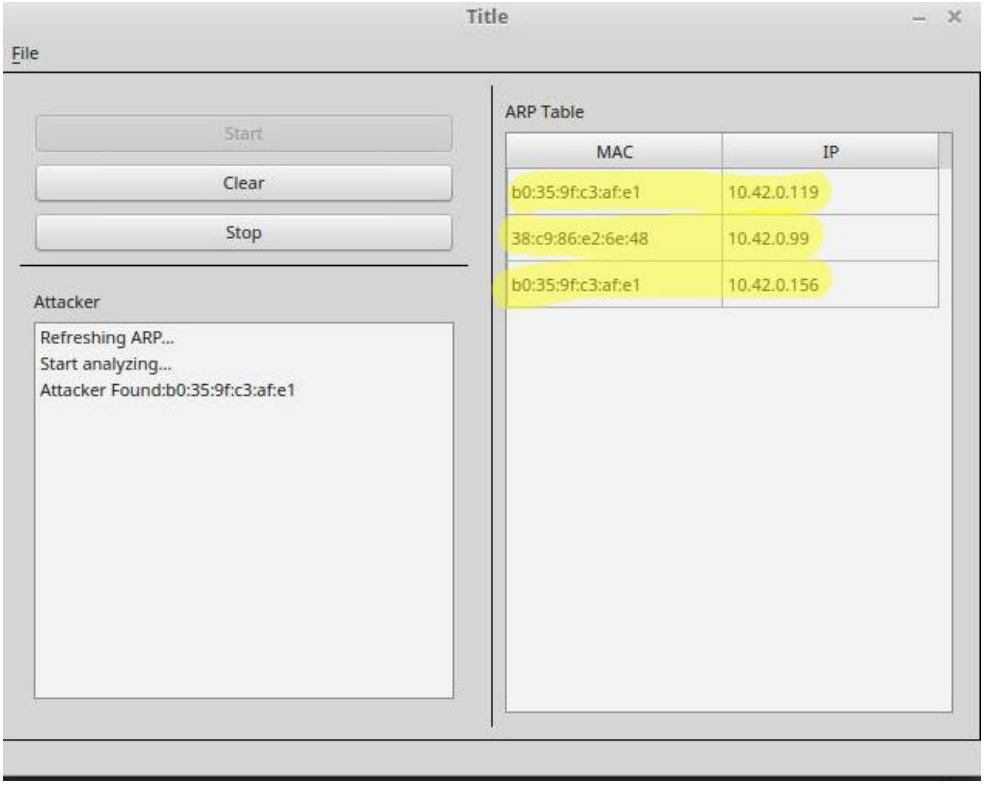
```
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fc Source MAC : 58:00:e3:73:18:e3 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : cc:fd:17:eb:de:22 Protocol : 8
Destination MAC : 00:c2:c6:4e:16:05 Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:02 Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 54:8c:a0:a3:d3:21 Protocol : 8
```

DETECTED NODE # 4

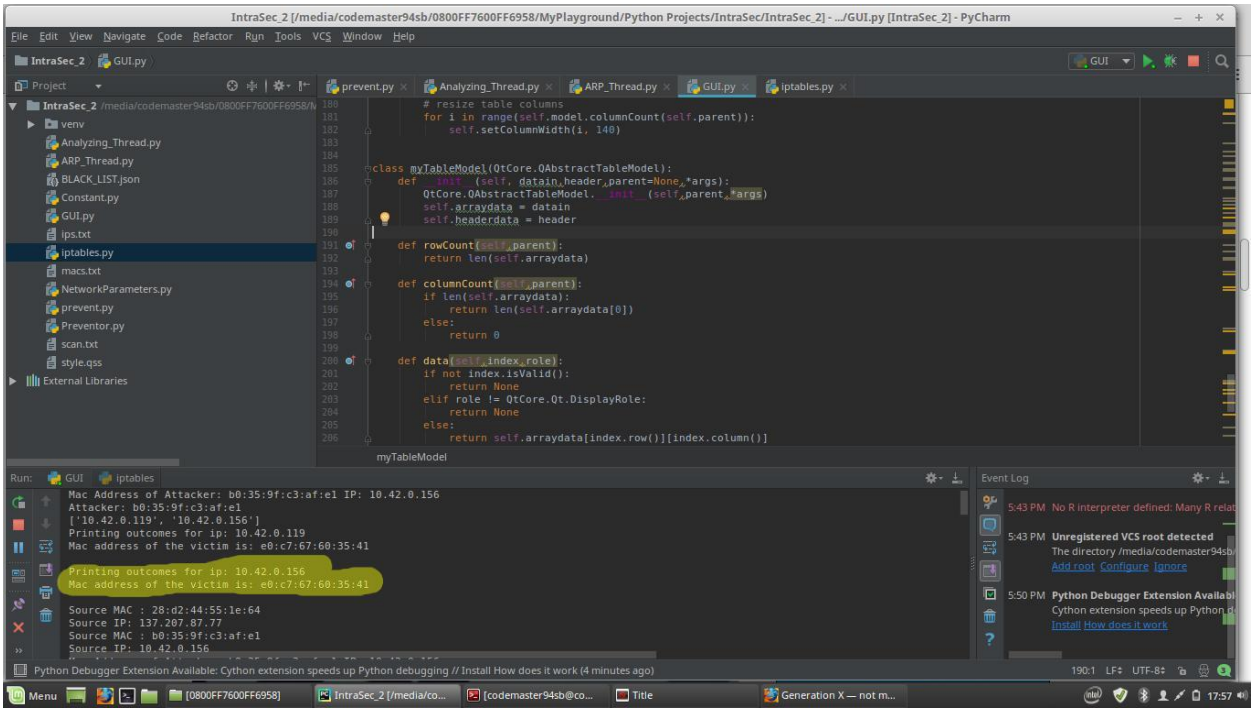
```
Destination MAC : 01:00:5e:00:00:fb Source MAC : cc:fd:17:eb:de:22 Protocol : 8
Destination MAC : 00:c2:c6:4e:16:05 Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:02 Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:7f:ff:fa Source MAC : 54:8c:a0:a3:d3:21 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
Destination MAC : 01:00:5e:00:00:fb Source MAC : e0:c7:67:60:35:41 Protocol : 8
```

D. Maintaining ARP table:





E. Identifying Victim:



F. Tracing the Attacker (Comparing IP and MAC addresses):

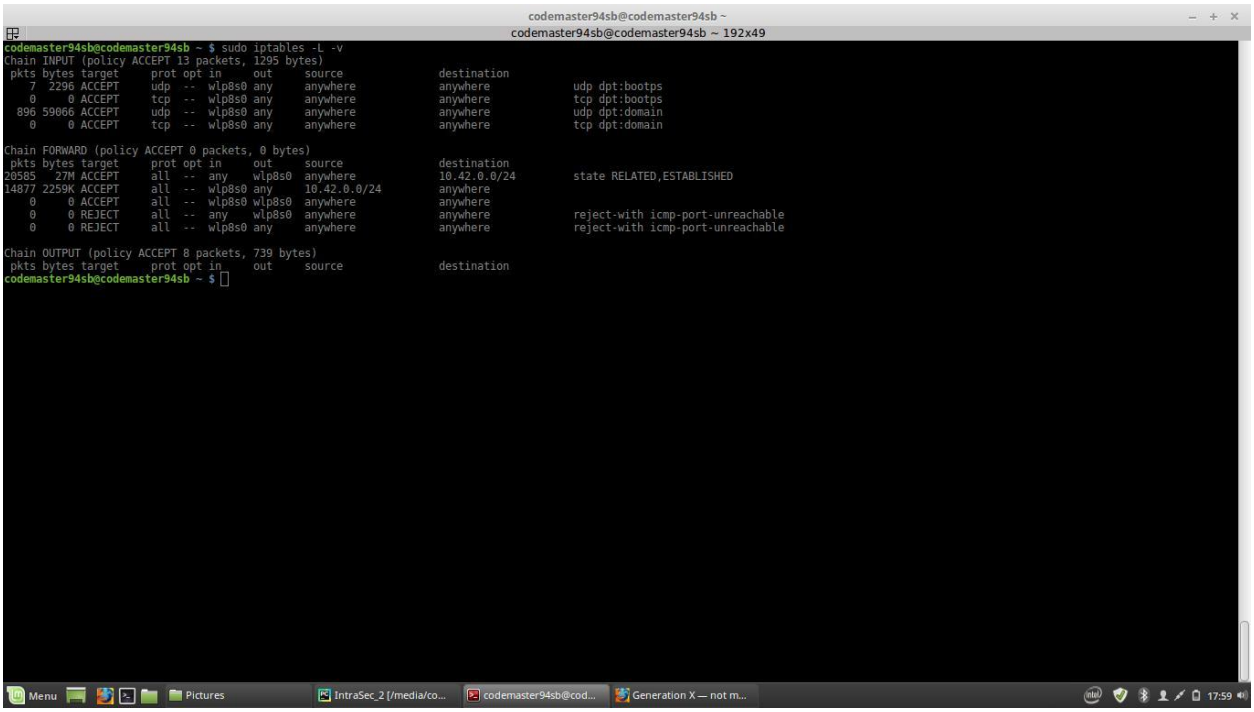


Fig: Network in initial stage

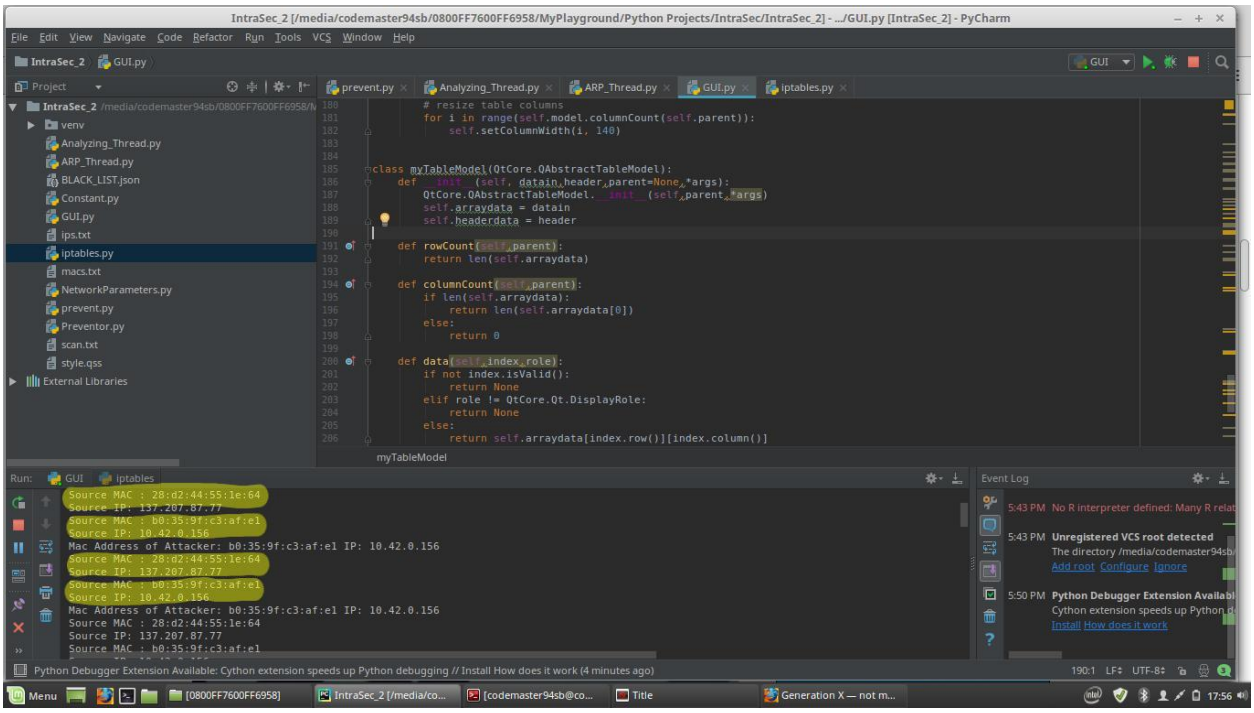
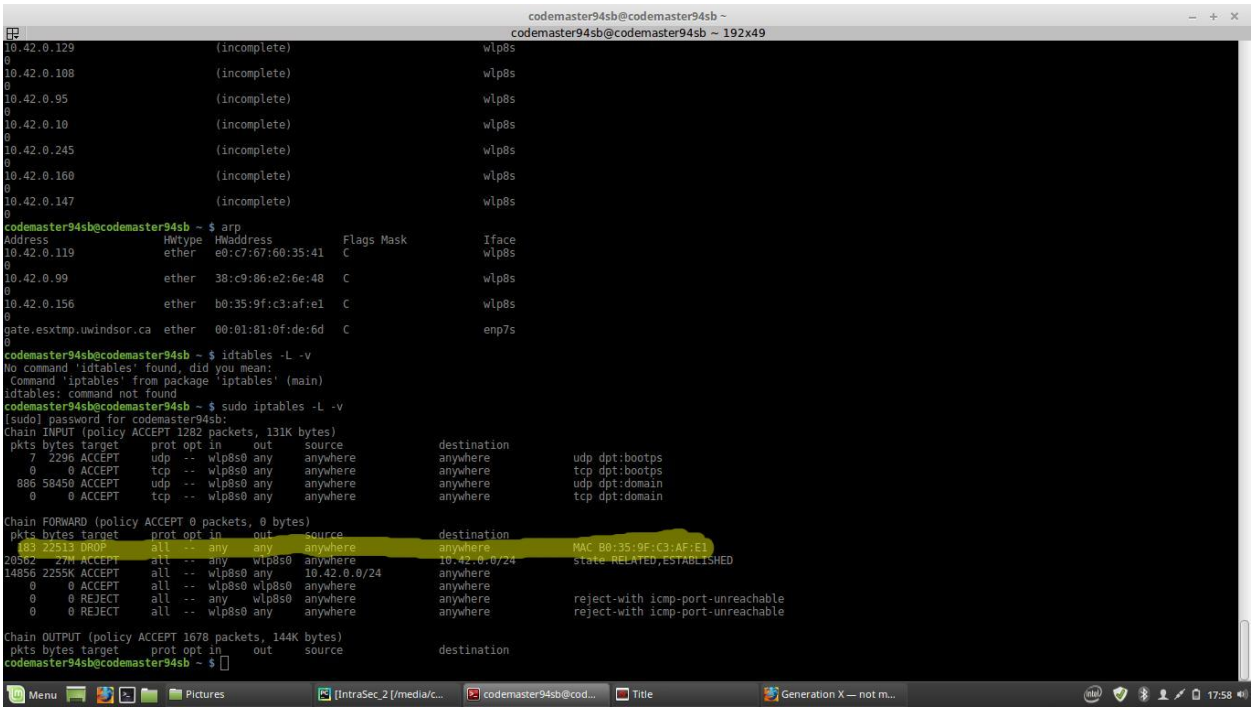


Figure: Scanning Network

G. Block and discard the packets corresponding to detected attacker machine:



H. References:

1. Jinhua G, Kejian X. ARP spoofing detection algorithm using ICMP protocol. InComputer Communication and Informatics (ICCCI), 2013 International Conference on 2013 Jan 4 (pp. 1-6). IEEE.
2. Kwan P, inventor; Foundry Networks LLC, assignee. System and method for ARP anti-spoofing security. United States patent US 8,006,304. 2011 Aug 23.
3. Pandey P. Prevention of ARP spoofing: A probe packet based technique. InAdvance Computing Conference (IACC), 2013 IEEE 3rd International 2013 Feb 22 (pp. 147-153). IEEE.
4. Shakshuki EM, Kang N, Sheltami TR. EAACK—a secure intrusion-detection system for MANETs. IEEE transactions on industrial electronics. 2013 Mar;60(3):1089-98.
5. Bao F, Chen R, Chang M, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management. 2012 Jun;9(2):169-83.
6. Fossi M, Egan G, Haley K, Johnson E, Mack T, Adams T, Blackbird J, Low MK, Mazurek D, McKinney D, Wood P. Symantec internet security threat report trends for 2010. Volume XVI. 2011 Apr.
7. Binder Y, inventor; May Patents Ltd, assignee. System and method for routing-based internet security. United States patent US 9,177,157. 2015 Nov 3.
8. Robles RJ, Balitanas M, Kim TH. Security encryption schemes for internet SCADA: comparison of the solutions. InSecurity-Enriched Urban Computing and Smart Grid 2011 (pp. 19-27). Springer, Berlin, Heidelberg.
9. Yassir A, Ismaeel AA. Current Computer Network Security Issues/Threats. International Journal of Computer Applications. 2016;155(1).
10. Cerrudo C, Apa L. Hacking Robots Before Skynet1. IOActive Website. 2017.
11. Tang A. Hacking Back against Cyber Attacks. Chicago Policy Review (Online). 2015 Jul 21.
12. Prathibha PG, Dileesh ED. Design of a hybrid intrusion detection system using snort and hadoop. International Journal of Computer Applications. 2013 Jan 1;73(10).
13. Berthier R, Sanders WH. Specification-based intrusion detection for advanced metering infrastructures. InDependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on 2011 Dec 12 (pp. 184-193). IEEE.
14. Albin E, Rowe NC. A realistic experimental comparison of the Suricata and Snort intrusion-detection systems. InAdvanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on 2012 Mar 26 (pp. 122-127). IEEE.
15. Davidoff S, Ham J. Network forensics: tracking hackers through cyberspace. Upper Saddle River: Prentice hall; 2012 Jun 18.
16. Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of service attacks in wireless networks: The case of jammers. IEEE Communications surveys & tutorials. 2011 May;13(2):245-57.
17. Tegeler F, Fu X, Vigna G, Kruegel C. Botfinder: Finding bots in network traffic without deep packet inspection. InProceedings of the 8th international conference on Emerging networking experiments and technologies 2012 Dec 10 (pp. 349-360). ACM.
18. https://null-byte.wonderhowto.com/how-to/build-arp-scanner-using-scapy-and-python-0162731/
19. Duffy C. Learning Penetration Testing with Python. Packt Publishing Ltd; 2015 Sep 30.