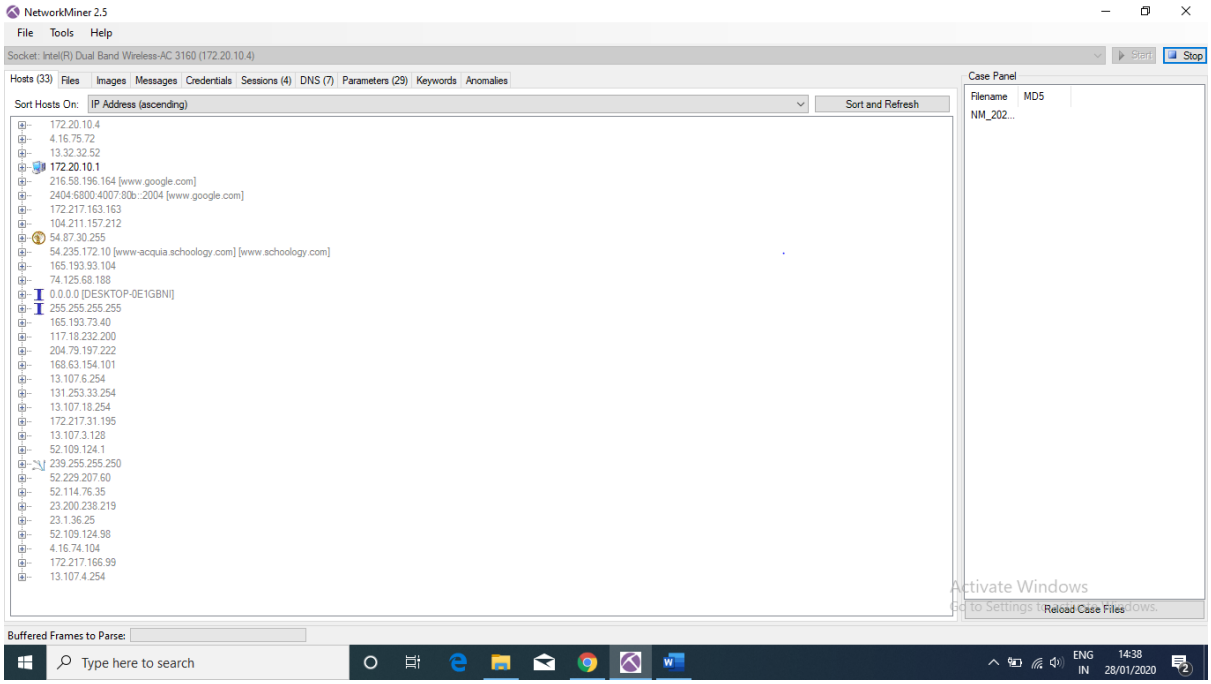
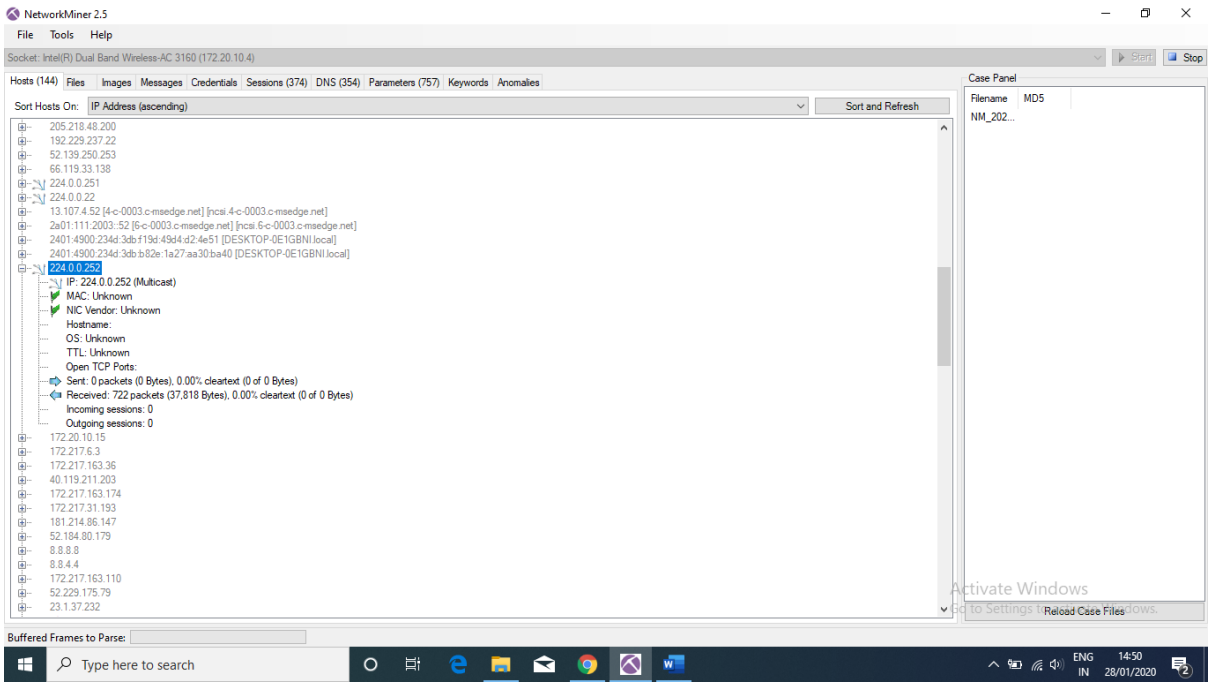
WINTER SEMESTER 2019-20
DIGITAL FORENSICS (CSE4004)
LAB ASSIGNMENT – 4

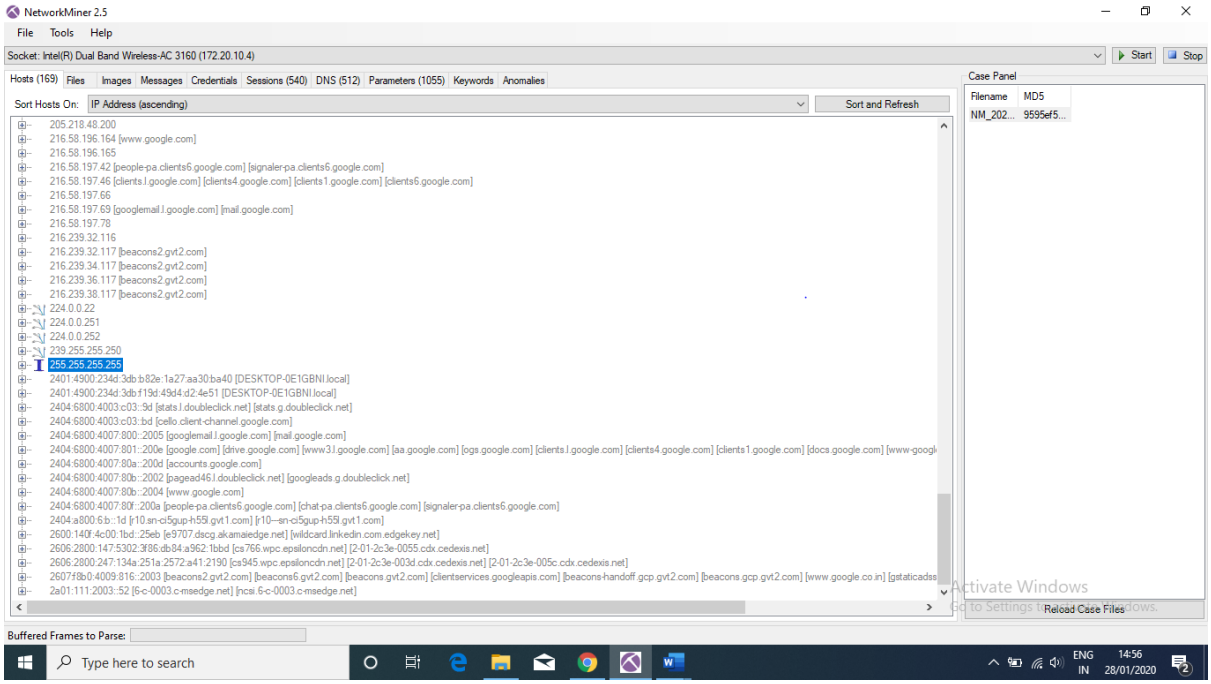
Dishi Jain
17BCB0055

Digital Forensics tool: NetworkMiner

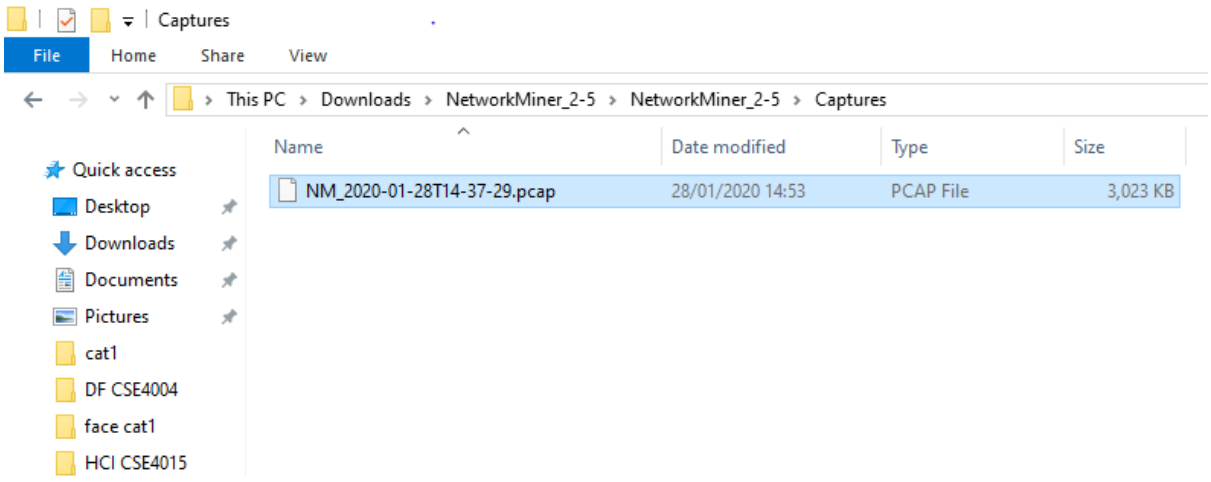
- NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). It can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. It collects data (such as forensic evidence) about hosts on the network rather than to collect data regarding the traffic on the network.
- NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.


NetworkMiner 2.5
File Tools Help
Socket: Intel(R) Dual Band Wireless-AC 3160 (172.20.10.4)
Start Stop
Hosts (33) Files Images Messages Credentials Sessions (4) DNS (7) Parameters (29) Keywords Anomalies
Sort Hosts On: IP Address (ascending) Sort and Refresh
172.20.10.4
4.16.75.72
13.32.32.52
172.20.10.1
216.58.196.164 [www.google.com]
2404:6800:4007:80b::2004 [www.google.com]
172.217.163.163
104.211.157.212
54.87.30.255
54.235.172.10 [www-acquia.schoology.com] [www.schoology.com]
165.193.93.104
74.125.68.188
0.0.0.0 [DESKTOP-0E1GBNI]
255.255.255.255
165.193.73.40
117.18.232.200
204.79.197.222
168.63.154.101
13.107.6.254
131.253.33.254
13.107.18.254
172.217.31.195
13.107.3.128
52.109.124.1
239.255.255.250
52.229.207.60
52.114.76.35
23.200.238.219
23.1.36.25
52.109.124.98
4.16.74.104
172.217.166.99
13.107.4.254
Case Panel
Filename MD5
NM_202...
Reload Case Files
Activate Windows
Buffered Frames to Parse:
Type here to search
ENG IN 14:38 28/01/2020


NetworkMiner 2.5
File Tools Help
Socket: Intel(R) Dual Band Wireless-AC 3160 (172.20.10.4)
Start Stop
Hosts (144) Files Images Messages Credentials Sessions (374) DNS (354) Parameters (757) Keywords Anomalies
Sort Hosts On: IP Address (ascending) Sort and Refresh
205.218.48.200
192.229.237.22
52.139.250.253
66.119.33.138
224.0.0.251
224.0.0.22
13.107.4.52 [4-c-0003.c-msedge.net] [ncsi.4-c-0003.c-msedge.net]
2a01:111:2003::52 [6-c-0003.c-msedge.net] [ncsi.6-c-0003.c-msedge.net]
2401:4900:234d:3db:f19d:49d4:d2:4e51 [DESKTOP-0E1GBNI.local]
2401:4900:234d:3db:b82e:1a27:aa30:ba40 [DESKTOP-0E1GBNI.local]
224.0.0.252
IP: 224.0.0.252 (Multicast)
MAC: Unknown
NIC Vendor: Unknown
Hostname:
OS: Unknown
TTL: Unknown
Open TCP Ports:
Sent: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 722 packets (37,818 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 0
172.20.10.15
172.217.6.3
172.217.163.36
40.119.211.203
172.217.163.174
172.217.31.193
181.214.86.147
52.184.80.179
8.8.8.8
8.8.4.4
172.217.163.110
52.229.175.79
23.1.37.232
Case Panel
Filename MD5
NM_202...
Reload Case Files
Activate Windows
Buffered Frames to Parse:
Type here to search
ENG IN 14:50 28/01/2020


NetworkMiner 2.5
File Tools Help
Socket: Intel(R) Dual Band Wireless-AC 3160 (172.20.10.4)
Start
Stop
Hosts (169) Files Images Messages Credentials Sessions (540) DNS (512) Parameters (1055) Keywords Anomalies
Case Panel
Filename MD5
Sort Hosts On: IP Address (ascending)
Sort and Refresh
205.218.48.200
216.58.196.164 [www.google.com]
216.58.196.165
216.58.197.42 [people-pa.clients6.google.com] [signaler-pa.clients6.google.com]
216.58.197.46 [clients.l.google.com] [clients4.google.com] [clients1.google.com] [clients6.google.com]
216.58.197.66
216.58.197.69 [googlemail.l.google.com] [mail.google.com]
216.58.197.78
216.239.32.116
216.239.32.117 [beacons2.gvt2.com]
216.239.34.117 [beacons2.gvt2.com]
216.239.36.117 [beacons2.gvt2.com]
216.239.38.117 [beacons2.gvt2.com]
224.0.0.22
224.0.0.251
224.0.0.252
239.255.255.250
255.255.255.255
2401:4900:234d:3db:b82e:1a27:aa30:ba40 [DESKTOP-0E1GBNI.local]
2401:4900:234d:3db:f19d:49d4:d2:4e51 [DESKTOP-0E1GBNI.local]
2404:6800:4003:c03::9d [stats.l.doubleclick.net] [stats.g.doubleclick.net]
2404:6800:4003:c03::bd [cello.client-channel.google.com]
2404:6800:4007:800::2005 [googlemail.l.google.com] [mail.google.com]
2404:6800:4007:801::200e [google.com] [drive.google.com] [www3.l.google.com] [aa.google.com] [ogs.google.com] [clients.l.google.com] [clients4.google.com] [clients1.google.com] [docs.google.com]
2404:6800:4007:80a::200d [accounts.google.com]
2404:6800:4007:80b::2002 [pagead46.l.doubleclick.net] [googleads.g.doubleclick.net]
2404:6800:4007:80b::2004 [www.google.com]
2404:6800:4007:80f::200a [people-pa.clients6.google.com] [chat-pa.clients6.google.com] [signaler-pa.clients6.google.com]
2404:a800:6:b::1d [r10.sn-ci5gup-h55l.gvt1.com] [r10---sn-ci5gup-h55l.gvt1.com]
2600:140f:4c00:1bd::25eb [e9707.dscg.akamaiedge.net] [wildcard.linkedin.com.edgekey.net]
2606:2800:147:5302:3f86:db84:a962:1bbd [cs766.wpc.epsiloncdn.net] [2-01-2c3e-0055.cdx.cedexis.net]
2606:2800:247:134a:251a:2572:a41:2190 [cs945.wpc.epsiloncdn.net] [2-01-2c3e-003d.cdx.cedexis.net] [2-01-2c3e-005c.cdx.cedexis.net]
2607:f8b0:4009:816::2003 [beacons2.gvt2.com] [beacons6.gvt2.com] [beacons.gvt2.com] [clientservices.googleapis.com] [beacons-handoff.gcp.gvt2.com] [beacons.gcp.gvt2.com] [www.google.co.in]
2a01:111:2003::52 [6-c-0003.c-msedge.net] [ncsi.6-c-0003.c-msedge.net]
Activate Windows
Reload Case Files
Buffered Frames to Parse:
Type here to search
ENG
IN
14:56
28/01/2020

pcap file


Captures
File Home Share View
This PC › Downloads › NetworkMiner_2-5 › NetworkMiner_2-5 › Captures
Quick access
Desktop
Downloads
Documents
Pictures
cat1
DF CSE4004
face cat1
HCI CSE4015
Name
Date modified
Type
Size
NM_2020-01-28T14-37-29.pcap
28/01/2020 14:53
PCAP File
3,023 KB