Network Forensic Report

PCAP Network Packet Capture Analysis

Last compiled by Sriram Raghavan
On the date 5/22/2008

This report provides the details of the forensic analysis performed on the network capture file "nforensics.pcap" in Brisbane, Queensland Australia

Table of Contents

1. Executive Summary 3
2. Introduction 4
   2.1 Network Capture File details 4
   2.2 Network Components Identified 5
3. Methodology 6
   3.1 Tools Used 6
   3.2 Steps Involved 6
   3.3 Handling Data 7
4. Detailed Findings 8
   4.1 Important network players 8
   4.2 Network Structure 9
   4.3 Activity Timeline for 192.168.1.103 10
   4.4 Background evidence 10
5. Supporting Evidence Presented 16
6. Conclusions 17
7. Appendix A – List of figures 19
   Evidence 038 19
   Evidence 039 20
   Evidence 040 21
   Evidence 041 22
   Evidence 042 23
   Evidence 043 24
   Evidence 044 25

©Secure Cyber Space 2012

1. Executive Summary

The purpose of this report is to analyse and report the contents of a network capture file nforensics.pcap.gz which is an archive containing the network based activities monitored on a given network. This file was extracted to **nforensics.pcap** file on a local hard drive before carrying out the analysis. The network is reported to contain the activities of an individual operating with an IP address 192.168.1.103 on a host network. The analysis attempts to reconstruct the structure of the network, identify key players in the network and determine all activities leading to and occurring during the reported malicious activity. The analysis was carried out mainly using network forensic tools such as Wireshark ver0.99.7 and pyFLAG ver0.86RC1. Some key findings from the analysis are listed below. Each of these findings has been elaborated with supporting evidence documents in Section 4.4.

1. There are 6 active components on the 192.168.1.xx subnet. The known IPs are 192.168.1.1, 192.168.1.103, 192.168.1.105 and 192.168.1.121.
2. Two devices with MAC addresses UscInfor-00-00-02 and UscInfor-00-00-FB did not actively participate in the conversations and can be regarded as irrelevant to the case.
3. The IP 192.168.1.1 directs several requests to external domains and it is identified as a Cisco Router on the subnet.
4. Based on the DNS response analysis, the suspect seems to be residing in Australia or New Zealand.
5. The suspect computer runs Windows NT 5.1 operating system with Mozilla Firefox 1.5.0.7 browser.
6. Based on the machine name of the suspect's computer LAMONT01 and the MSN Hotmail ID lam3rallround@hotmail.com, the suspect's name may be Lamont.
7. The suspect has searched for and obtained a copy of WGET.exe downloaded from http://users.ugent.be/~bpuype/wget.
8. The suspect was found to have logged into the router and reconfigured the firewall.
9. During the analysis, the following email IDs were observed:
    a. lam3rallround@hotmail.com
    b. phlatoutphishing@yahoo.com.au
    c. gonnagetphished@gmail.com
10. The suspect owns the ID lam3rallround@hotmail.com and uses MSN messenger ver7.5.0299 for chat sessions.
11. The suspect's accomplice with Yahoo ID phlatoutphishing@yahoo.com.au was IDed as Mr. Justin Case
12. Based on the chat sessions analysed, the suspect (lam3rallround@hotmail.com) and Mr. Justin Case (phlatoutphishing@yahoo.com.au) were planning to mirror the National Australia Bank (NAB) and use the mirror as a phishing website.The suspect and Mr. Justin Case send a phishing email to Mr. Ronald Brown with Google Mail ID gonnagetphished@gmail.com

©Secure Cyber Space 2012

13. Mr. Justin Case tells the suspect that the phishing website captures bank account and password details before forwarding to the real bank website.
14. Searching through the strings output file for the search string "password" revealed that the phishing website had captured Mr. Ronald Brown account details with NAB
    a. Account Number: *408854893*
    b. Password: *96Cam*
15. The filter `ip.addr == 220.237.83.151` revealed no transactions with suspect's IP 192.168.1.103. However, there is a sequence of transactions between the suspect's IP and 165.228.133.11 and 200.88.223.98 on port 31337. This is suspicious and the investigator believes that the suspect has tunnelled the access bypassing the firewall on router 192.168.1.1 to 220.237.83.151 on the same port.

2. Introduction

2.1 Network Capture File details

The extracted PCAP network capture file nforensics.pcap has the forensic parameters as given below. The evidence for these details is provided in Figure 1 extracted from Wireshark ver0.99.7:

Capture length:	10709492 bytes
Format:	Wireshark/tcpdump/... – libpcap
Packet size limit:	65535 bytes
First packet:	08-OCT-2006 14:09:59 HRS
Last packet:	08-OCT-2006 16:27:38 HRS
Elapsed time:	2 hours, 17 minutes, 38 seconds (8258.972 seconds)
Total packets:	16, 263
Average packets/sec	1.969 packets/sec
Average packet size	642.517 bytes
Average bytes/sec	1265.201 bytes/sec

Computed HASHes – nforensics.pcap.gz

MD5:	5E71542623C993F987E477A5ACD6CF9C
SHA1:	10D7EB58E57D2F7D19030F820BEDA7229B2009B6

©Secure Cyber Space 2012

Computed HASHes – nforensics.pcap

MD5: AC569D56768C6F827D24E74D4383BD6D (verified)

SHA1: 13047906924F6F0E7FA3FEE63285C16DF727FD34

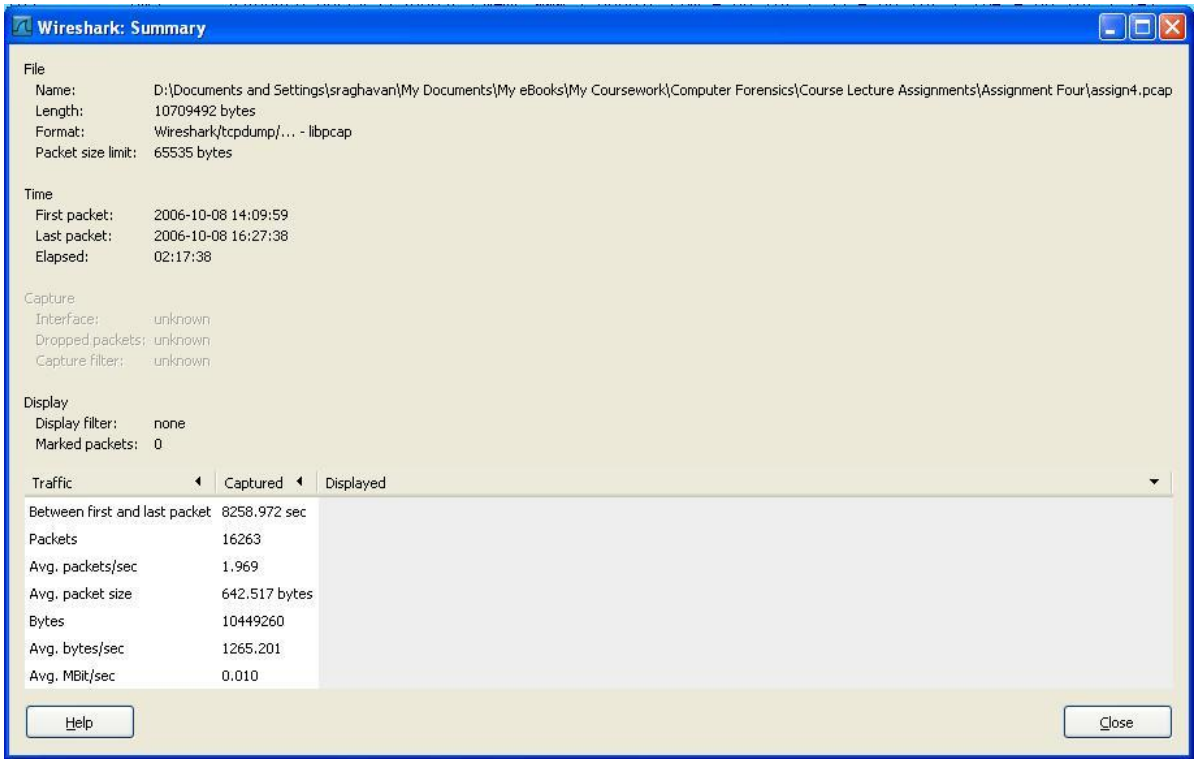


Figure 1. Packet capture summary from Wireshark ver0.99.7

2.2 Network Components Identified

According to the capture summary as provided by Wireshark ver0.99.7, there are 6 distinct Ethernet components. They were determined using the Ethernet Endpoints listed under Statistics as below:

1. AppleCom-78-F9-AF	192.168.1.121	Apple iBook G4 – laptop
2. AppleCom-9F-51-76	192.168.1.105	Apple Computer
3. AsustekC-8E-56-84	192.168.1.103	Windows NT 5.1 (en-GB)
4. Cisco-Li-2A-9F-46	192.168.1.1	Cisco Router
5. UscInfor-00-00-02		
6. UscInfor-00-00-FB		

Based on the statistics report, it appears that the devices UscInfor-00-00-02 and UscInfor-00-00-FB were not significantly involved in the conversations tracked on the network capture file and hence can be regarded irrelevant for the remaining part of the investigation. The device with MAC address AsustekC-8E-56-84 was found to have the IP address

©Secure Cyber Space 2012

192.168.1.103 which was our suspicious individual. Besides this, the device with MAC address Cisco-Li-2A-9F-46 was found to have the IP address 192.168.1.1. This device was also found to direct several packets from the suspect's IP address 192.168.1.103 to external websites such as Google Mail, Yahoo, MSN, and several others. This could potentially imply that this device was also functioning as a router in the network. Based on the evidence that there was a sequence of TCP transactions between 192.168.1.103 and 192.168.1.1, this report concludes that the router was also playing host to one or more application services.

3. Methodology

3.1 Tools Used

The analysis analysed the contents using network forensic tools such as Wireshark ver0.99.7 executing under Windows XP Service Pack 2 on 2.33GHz Intel Core 2 Duo CPU with 1.95 GB RAM and pyFLAG ver0.86RC1 executing on Fedora Linux platform running kernel 2.6.21 on the same system. The findings were later cross verified on another system 1.66 GHz Intel Core 2 Duo CPU with 2 GB RAM running Windows Vista Home Premium Service Pack 1 running Wireshark ver0.99.7. The analysis revealed several external IPs which were resolved using the NSLOOKUP tool connected to HELIOS.isi.qut.edu.au (IP 131.181. 6.4) as the primary DNS server. This was verified with the same service connected to SENTRY.isi.qut.edu.au (IP 131.181.97.10) server. There were several IP addresses that were unresolved by the DNS servers listed above given in Section 4, Table 3 of this report.

3.2 Steps Involved

The archive was extracted to nforensics.pcap and opened using the Wireshark ver0.99.7 tool in Windows for analysis. The preliminary details regarding the capture were extracted from the Statistics tab which provides the list of all endpoints and conversations taking place at the Ethernet, IP, TCP and UDP layers. The list revealed several external addresses that were resolved using the NSLOOKUP tool at various points during the analysis. Having performed this preliminary analysis, packet capture filters were applied to the Wireshark ver0.99.7 tool to trace transactions of a specific type. This allowed the analysis to focus on the specific aspects to determine the IPs that generated most traffic of a particular type. These filters are based on the syntax directed by the LIBPCAP library that governs the operations of the Wireshark tool. Some of the filters applied included –

IP, DNS, UDP, TCP, HTTP, SSL, MSNMS, IGMP, `ip.addr == 192.168.1.103`, `ip.src == 192.168.1.103`, `tcp && ip.dst == 192.168.1.103`, `ip.dst == 192.168.1.103`, `ip.addr == 192.168.1.1`, `http && ip.dst == 192.168.1.1`, etc.

pyFLAG was used to determine the text messages exchanged on the network between suspect (IP 192.168.1.103) and others. The chain of messages traced indicates that the suspect is guilty of attempting to mirror the National Australia Bank (www.national.com.au) and phish

the website. The suspects' accomplice is the messenger contact *phlatoutphishing@yahoo.com.au*. The two contacts plan on mirroring the bank's website and send a bogus email requesting personal contact information from a person known to hold an account with the same bank. Based on the communication, the NAB server was mirrored and hosted as a phishing website at 220.237.83.151; port 31337 by the accomplice. There is no explicit transaction record between 192.168.1.103 and 220.237.83.151 in PCAP file.

3.3 Handling Data

Wireshark: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	16263	10449260	0.010	0	0	
Ethernet	100.00%	16263	10449260	0.010	0	0	
Internet Protocol	99.32%	16153	10443974	0.010	0	0	
User Datagram Protocol	1.64%	266	52922	0.000	0	0	
Domain Name Service	1.38%	224	45594	0.000	224	45594	
EtherNet/IP (Industrial Protocol)	0.02%	3	448	0.000	0	0	
Malformed Packet	0.02%	3	448	0.000	3	448	
Data	0.06%	10	620	0.000	10	620	
Hypertext Transfer Protocol	0.01%	2	349	0.000	2	349	
Malformed Packet	0.03%	5	210	0.000	5	210	
NetBIOS Datagram Service	0.12%	20	5009	0.000	0	0	
SMB (Server Message Block Protocol)	0.12%	20	5009	0.000	0	0	
SMB MailSlot Protocol	0.12%	20	5009	0.000	0	0	
Microsoft Windows Browser Protocol	0.12%	20	5009	0.000	20	5009	
Bootstrap Protocol	0.01%	2	692	0.000	2	692	
Transmission Control Protocol	97.67%	15884	10390587	0.010	13446	9254834	
Hypertext Transfer Protocol	5.32%	866	494450	0.000	605	370548	
Line-based text data	0.33%	53	39277	0.000	53	39277	
Compuserve GIF	1.22%	198	79028	0.000	198	79028	
Portable Network Graphics	0.02%	3	2073	0.000	3	2073	
JPEG File Interchange Format	0.03%	5	1859	0.000	0	0	
Malformed Packet	0.03%	5	1859	0.000	5	1859	
Media Type	0.01%	2	1665	0.000	2	1665	
Secure Socket Layer	3.55%	578	253312	0.000	578	253312	
MSN Messenger Service	4.13%	671	108914	0.000	671	108914	
Data	1.99%	323	279077	0.000	323	279077	
Internet Control Message Protocol	0.01%	2	405	0.000	2	405	
Internet Group Management Protocol	0.01%	1	60	0.000	1	60	
Address Resolution Protocol	0.68%	110	5286	0.000	110	5286	

Figure 2. Protocol Hierarchy captured with Wireshark ver0.99.7

Packet Type	Number of packets	Requests	Technique	Responses	Technique
ARP	110	89	`Arp`	21	`arp`
IP	16153	-		-	
TCP	15884	Not calc.		Not calc.	
UDP	268	-		-	
DNS	224				
HTTP	1113	542	`http && ip.src == 192.168.1.xx - POST`	527	`http && ip.src != 192.168.1.xx -`

©Secure Cyber Space 2012

					continuation – dest unreachable
BROWSER	20	-		-	
SSL	647	64	ssl (client + server hello)	579	ssl (647 – 4 dest unreachable) – 64 hello
MSNMS	671	-		-	

Table 1. Decomposition of different packet types from capture

Based on the statistics given in table 1, the network was predominantly TCP traffic based. The Wireshark `tcp` filters reveal significant amount of TCP request responses to IP addresses 192.168.1.103 and 192.168.1.1. Since the machine with IP 192.168.1.1 appears to be a Cisco Router, this report concludes that 192.168.1.103 was the major contributor to this traffic. Besides, significant browsing has also been detected under Wireshark using the filter `http` to external websites which is cross verified with pyFLAG Network forensic analysis. Evidence is presented in Evidence File ID 12, 14 and 15 given in Section 5 Table 4 in this report.

IP Address	As Sender	As Receiver
192.168.1.103	6713	9437
192.168.1.1	231	213
192.168.1.121	5	0
192.168.1.105	0	0
192.168.1.111	0	0

Table 2. Decomposition of IP traffic (Inbound & Outbound)

It is evident from the information presented in Table 2 that 192.168.1.103 was the most prominent player in the network activity captured on 08th OCT 2006. Activity seen on the IP 192.168.1.1 can be attributed to its role as a router on the network.

4. Detailed Findings

4.1 Important network players

1. AppleCom-78-F9-AF 192.168.1.121 Apple iBook G4 – laptop
2. AppleCom-9F-51-76 192.168.1.105 Apple Computer
3. AsustekC-8E-56-84 192.168.1.103 Windows NT 5.1 (en-GB)
4. Cisco-Li-2A-9F-46 192.168.1.1 Cisco Router

In order to determine the IP addresses of the different MAC devices on the network, the investigator examined the source and destination addresses on the Ethernet and IP packets being exchanged over this network. This examination was then correlated with the findings between the two layers of source and destination addresses. This revealed that devices with MAC addresses AsustekC-8E-56-84, AppleCom-78-F9-AF and AppleCom-9F-51-76 owned

©Secure Cyber Space 2012

the IP addresses 192.168.1.103, 192.168.1.121 and 192.168.1.105 respectively. While the device with MAC address Cisco-Li-2A-9F-46 was detected with multiple IP addresses during this examination, NSLOOKUP service revealed that several IPs belonged to external domains and hence, this device must have acted as a router of the packets. As a result, this report confirms the identity of this device as a Cisco Router with IP address 192.168.1.1. Evidence is presented in Evidence File ID 1 – 9 and 38 – 41 given in Section 5 Table 4 of this report.

4.2 Network Structure

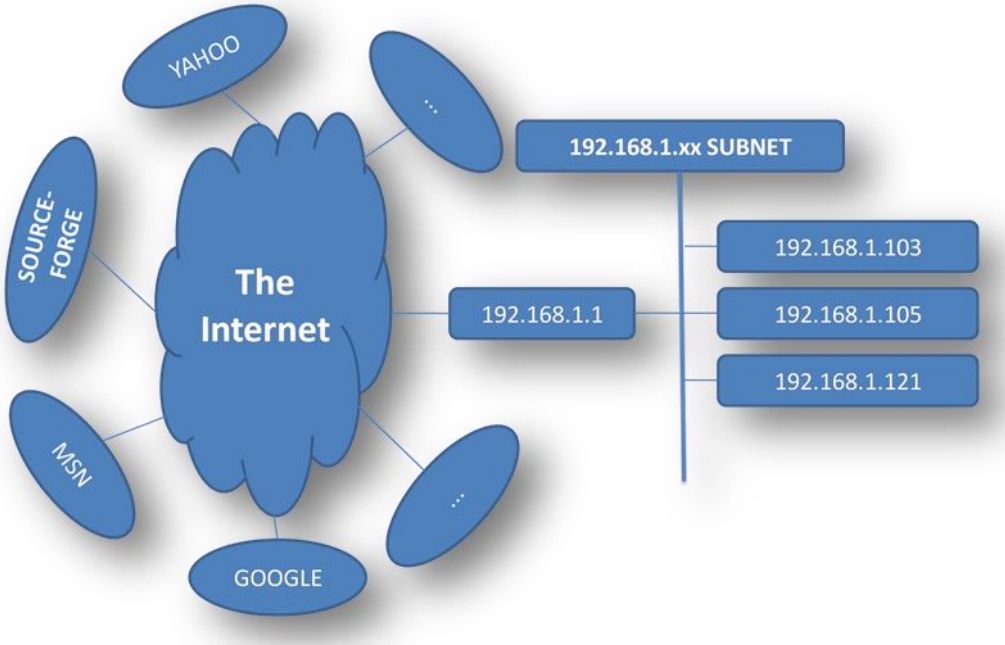


Figure 3. Possible Network Structure based on reconstruction from nforensics.pcap

Based on the forensic analysis of the packets captured, the possible network structure is illustrated in Figure 1. The several DNS requests directed to 192.168.1.1 indicates that this machine was a DNS server to the network. Besides, there are several external websites visited which at the MAC layer are directed through this machine in question. Hence, this report concludes that the machine was a Cisco Router. Based on the TCP transactions between this machine and suspect 192.168.1.103, this report infers that applications such as firewall.sh and cgi-bin/webif.sh have been running on this machine. This is observed by selecting the filter `tcp && ip.addr == 192.168.1.1` between packets numbered 6960 and 7189. The investigator opines that the machine was executing a firewall application to which suspect user had administrative access. It is unclear if the suspect acquired this access legally or illegally.

©Secure Cyber Space 2012

4.3 Activity Timeline for 192.168.1.103

Packet Number	Activity	Destination	Inference
1	Google Search, Australia	66.102.7.99	Searching for info
39, 81	Search result: how to mirror website	66.102.7.99	Seeking how to mirror websites
109	htdig.binarycompass.org	216.52.244.214	Seeking how to mirror websites
98	Search result: wget win32 binary	66.107.7.99	Searching for wget.exe
198	users.ugent.be/~bpuype/wget/	157.193.40.15	Attempting to download wget.exe
1023	ak.imgag.com	198.142.23.81	
1073	rad.msn.com	207.68.178.16	Logging into MSN mail server
1388	kiwi.planetmirror.com	203.16.234.91	Mirror site for download
6945	Google Search, Australia	66.102.7.99	Searching for info
6964	Cisco Router	192.168.1.1	Reconfiguring firewall
7213	NO LOOKUP	165.228.133.11	Tunnelled transactions to phishing website hosted at 220.237.8.151 on port 31337
7286	national.com.au	203.57.240.101	Mirroring NAB website
8091	forecastfox.accuweather.com	32.114.14.11	Searching for weather forecast – Brisbane
9887	au.yimg.com	198.142.23.22	Communicating with Yahoo messenger server
10728	yahoo.com	68.142.213.132	Communicating with Yahoo server
10790	yahoo.com	209.73.168.74	Communicating with Yahoo server
11607	NO LOOKUP	12.129.210.46	UNKNOWN
13386	codetel.net.do	200.88.223.98	Tunnelled transactions to phishing website hosted at 220.237.8.151 on port 31337
13596	national.com.au	203.57.241.101	Mirroring NAB website
14994	iprimus.net.au	210.50.7.243	UNKNOWN

Table 3. Activity Timeline based on network forensic analysis and event reconstruction

Note: Only distinct IP addresses with different time stamps are mentioned on the table. Each IP has a sequence of following TCP/HTTP packets following it which is not captured in this table. Packet numbers provided in the table indicate the first occurrence of the transaction.

4.4 Background evidence

1. The capture file is forensically secure verified by the MD5SUM of the uncompressed file against the report provided. Besides, the investigator has also secured this copy with the SHA1SUM of the same file. Refer to Section 2.1 for details.
2. All communication has taken place between 2:09:59 PM and 4:27:38 PM on OCT the 8th 2006. The evidence is presented in Section 2.1 on Network Capture File Details.
3. There are 6 active components on the 192.168.1.xx subnet of which one of them is a Cisco router (IP 192.168.1.1) and one is the wanted suspect (IP 192.168.1.103) computer running Windows NT 5.1 and one is an Apple G4 iBook laptop (IP 192.168.1.121). We infer this information by selecting `Endpoints` in `Statistics` tab and correlating this information with the ARP packets using `arp`

©Secure Cyber Space 2012

filter in Wireshark ver0.99.7. Evidence ID 1 and 2 given in Table 4 give a list of all Ethernet conversations and endpoints detected in the network and Evidence ID 3 gives the list of ARP traffic in the network.

4. Using the filter `dns && ip.src == 192.168.1.121` reveals exactly one packet to destination 224.0.0.251. The info contents of this packet indicate that the source machine (IP 192.168.1.121) is an Apple iBook G4 which is an Apple Laptop computer. Evidence ID 18 in Table 4 providing the list of DNS queries is provided in support of this argument.
5. Using the `arp` filter in Wireshark ver0.99.7 and by selecting the `Endpoints` in `Statistics` tab, this report observes that the number of packets transmitted from them is negligible. This report concludes that the devices with MAC addresses UscInfor-00-00-02 and UscInfor-00-00-FB did not participate actively in the network. Evidence ID 2 and 3 in Table 4 are presented in support of this argument.
6. The filters `ip.dst == 192.168.1.105` and `ip.dst == 192.168.1.121` reveal no packets on Wireshark which leads this report to believe that these machines did not receive any packets during the period. This was verified with pyFLAG by browsing thru the virtual file system using the inbuilt network filters.
7. The filter `ip.src == 192.168.1.105` reveals no packets and this indicates that this machine did not actively participate in the network.
8. The filter `ip.src == 192.168.1.121` reveals exactly 5 packets of which none are of suspicious nature. These are routine ENIP packets (broadcast) and one IGMP packet requesting to leave group. This report concludes that this machine also did not actively participate in the network during the period of network capture.
9. Using the filter `dns && ip.addr == 192.168.1.105` and `dns && ip.addr == 192.168.1.105` does not reveal packets which would indicate that these machines hosted any application services. In other words, no server applications were detected on these machines.
10. Using the `dns` filter, the packets reveal several DNS requests directed to 192.168.1.1. Besides, most of these requests have originated from the suspect computer. We infer that a DNS service was executing on 192.168.1.1 and the suspect has visited several external websites. Evidence ID 18 in Table 4 lists the DNS queries in the network.
11. The filter `tcp && ip.addr == 192.168.1.1` reveals several transactions between 192.168.1.1 and 192.168.1.103. On analysing the contents of these packets (analysis of the HTTP/1.1 GET packets), this report observes that applications including `firewall.sh` and `cgi-bin/webif.sh` have been executing on 192.168.1.1. This report believes that 192.168.1.1 has been executing a firewall that was reconfigured by the suspect. Evidence ID 20 and 21 in Table 4 listing the TCP requests and responses exchanged between 192.168.1.1 and 192.168.1.103 are presented in supported of this argument.
12. Using the filter `http && ip.src == 192.168.1.103` and analysing the HTTP/1.1 GET packets reveal that the HTTP User agent is Mozilla Firefox 1.5.0.7 browser. Further, most responses direct the browser to Australian websites. This indicates that the subnet may be present in Australia or New Zealand. This implies

©Secure Cyber Space 2012

that the suspect (192.168.1.103) is residing in Australia or New Zealand. Evidence ID 14 in Table 4 listing the HTTP requests generated from 192.168.1.103 is presented in evidence. Evidence ID 23 and 23 providing the load analysis on the network support this argument.

13. The suspect visits several external websites including Google mail, Yahoo, Live Messenger, etc. There are several IP addresses directed through 192.168.1.1 which NSLOOKUP shows are belonging to external sites. This information can be correlated with packets displayed using filter `dns && ip.addr == 192.168.1.103`. There is one-to-one correspondence between the number of requests to external websites generated by suspect to router and the DNS responses back to suspect. Evidence ID 18 in Table 4 filtered with Source IP 192.168.1.103 is presented in evidence. Evidence ID 23 and 23 providing the load analysis on the network support this argument.
14. Based on the search of strings from Evidence ID 10 in Table 4, the following information is available about the suspect's cookie at the Google Australia server:
    a. Windows NT 5.1 en-GB
    b. Gecko/20060909 Firefox/1.5.0.7
    c. PREF_ID – 0c44975525448bce
    d. TM – 1067755592
    e. LM – 1067755593
    f. S – GmLb8HCXA5UevkgY
15. The suspect has attempted to search for "*how to mirror website*" recovered from the pyFLAG network forensic analysis using HTTP filters. Evidence ID 12 in Table 4 listing the contents of the HTTP transactions is presented in evidence. Evidence can also be obtained from Evidence ID 18 searching for DNS requests to Google Search with search strings "*how to mirror website*".
16. The frequency of multiple DNS requests generated within a short span of time (several instances detected) using the filter `dns && ip.addr == 192.168.1.103` indicates that the suspect was running several parallel sessions of the browser simultaneously. It is unclear whether these sessions were generated from multiple different browser windows or the same browser windows with multiple tabbed sessions. Evidence ID 18 in Table 4 is presented in evidence.
17. The suspect has attempted to search for "*wget win32 binary*" recovered from the pyFLAG network forensic analysis using HTTP filters. Evidence ID 12 in Table 4 listing the contents of the HTTP transactions is presented in evidence. Evidence can also be obtained from Evidence ID 18 searching for DNS requests to Google Search with search strings "*wget win32 binary*".
18. The sequence of several requests to websites such as addons.mozilla.org, www.fsf.org, www.apache.org, fpdownload.macromedia.com, titus.planetmirror.com indicate that the browser used by the suspect was being updated dynamically by downloading active contents to display web pages. Correlating this information with the MSN chat sessions, it indicates that the suspect was searching for GNU WGET.EXE tool which is used to download content from the Internet over

©Secure Cyber Space 2012

HTTP/HTTPS/FTP protocols. Evidence ID 18 and 19 listing the DNS queries and responses are provided in evidence.

19. Based on the HTTP request analysis and the NSLOOKUP service, the suspect has also spent considerable time on browsing thru the Akamai Technologies webpage (http://ak.imgag.com and http://deploy.akamaitechnologies.com). However, when the investigator visited these web pages, the content indicated the presence of a GIF file which could not be displayed in either Mozilla Firefox or Internet Explorer on the investigator's machine.
20. Using the filter `browser && ip.src == 192.168.1.103`, the packets displayed contain the NetBIOS Datagram service which lists the source name as LAMONT01 Workstation/Redirector. The name of the machine may contain some clues to the name of the user (suspect) of this computer.
21. The filter `msnms` displays the packets using this protocol to communicate using MSN instant messenger. Evidence ID 11 in Table 4 listing the contents of the MSN chat conversations between the suspect (IP 192.168.1.103) and Yahoo ID phlatoutphishing@yahoo.com.au is presented in evidence. Examining the MSN messenger service contents shows the existence of at least one chat session during the capture. Further, the parties involved indicate that the communication is between the suspect and external websites. Chat stream contents contained in Evidence ID 26 – 37 in Table 4 support this argument.
22. The behaviour observed above indicates that the suspect has been actively communicating with other parties on the Internet. The NSLOOKUP service showed that the external website addressed belonged to YAHOO, GOOGLE, MSN MESSENGER and PHX.GBL domains. Based on some further verification, PHX.GBL was also found to belong to MSN MESSENGER domain. Besides, the service was also unable to reference few websites which can be attributed to dynamic IP address allocation employed on several domain servers for load balancing.
23. The NSLOOKUP results returned for several MSN web services are different from the data determined from the analysis using Wireshark ver0.99.7. These were not detected by the Network level Name resolution protocol used internall by Wireshark ver0.99.7 or by pyFLAG 0.86RC1
24. During the analysis, the following messenger clients were communicating detected on the MSNMS protocol in Wireshark:
    a. lam3rallround@hotmail.com
    b. phlatoutphishing@yahoo.com.au
    c. Besides, there is a reference to a particular individual known to the suspect having an account with NAB. The suspect and his accomplice send a phishing email to this individual with email ID gonnagetphished@gmail.com

    Evidence for the first two discoveries is presented in Evidence ID 16 and 17 in Table 4 listing the incoming and outgoing MSN chat conversations and the third discovery is observed by search Evidence ID 10 for the "*phlatoutphishing*"

©Secure Cyber Space 2012

25. The suspect owns the ID lam3rallround@hotmail.com and uses MSN messenger ver7.5.0299 for chat sessions. This is discovered by analysing the MSN message packets in Wireshark ver0.99.7 using `msnms` filter and checking the `Info` contents of the packets. This is also confirmed as displayed in the `strings` output of the capture file. Evidence ID 16 and 17 in Table 4 are presented in evidence. Chat stream contents contained in Evidence ID 26 – 37 in Table 4 support this argument.
26. Based on the chat session analysis, there doesn't appear to be any talk sessions established while chatting over the messenger chat session. Evidence ID 16 and 17 in Table 4 are presented in evidence.
27. Based on the chat sessions analysed, the suspect (lam3rallround@hotmail.com) and an accomplice (phlatoutphishing@yahoo.com.au) were planning to mirror the National Australia Bank (NAB) and use the mirror as a phishing website. The TCP/HTTP sessions tracked indicate that the suspect has spent significant effort in mirroring the website and reconfiguring the router for this task. Based on the analysis, it appears that the suspect (lam3rallround@hotmail.com) modified the firewall configurations to grant access to the phishing website hosted by his accomplice (phlatoutphishing@yahoo.com.au). The actual hosting is done on latter's machine with IP 220.237.83.151; port: 31337. Evidence ID 11 listing the MSN chat contents between lam3rallround@hotmail.com and phlatoutphishing@yahoo.com.au is presented in evidence. Chat stream contents contained in Evidence ID 26 – 37 in Table 4 support this argument.
28. Using the filter `ip.addr == 220.237.83.151` interestingly revealed no packets. It is possible that this address bypassed the router (if this is at all possible) based on the router firewall reconfiguration the suspect had performed.
29. Based on this IP address, the investigator searched using the filter `tcp.port == 31337` which revealed two transaction sequences from suspect's IP 192.168.1.103 with IP addresses 165.228.133.11 and 200.88.223.98. This indicated that the suspect was operating these services from the port 31337 which showed up as destination ports in Wireshark ver0.99.7.
30. While searching the strings output file for the search string "*31337*", the search returned several HTTP GET requests directed to 220.237.83.151 on port 31337. This was very suspicious and the investigator believes that the suspect reconfigured the router 192.168.1.1 to tunnel all requests on 192.168.1.103 on port 31337 to the phishing website hosted on 220.237.83.151 on port 31337. Evidence is presented in Evidence ID 10 searching for the search string 31337.
31. It was determined that the IP 165.228.133.11 transacting with 192.168.1.103 on port 31337 executed a Macintosh OS X with Mozilla Firefox 1.5.05.
32. The two suspects also send out an email to an individual who they know holds an account with NAB. The individual was determined to have a Google Mail account with ID gonnagetphished@gmail.com. Evidence is presented in Evidence ID 10 in Table 4 by searching for "*gonnagetphished*" and "*phlatoutphishing*"
33. Based on the machine name LAMONT01 and the suspect's MSN Hotmail ID lam3rallround@hotmail.com, this report believes that the suspect may have a name

©Secure Cyber Space 2012

(first or middle or last) as Lamont. This report suggests that investigations run the records past people with the name Lamont having prior criminal record for an ID hit.

34. Having determined the contact IDs, the investigator performed a search on the string "*gonnagetphished*" and "*phlatoutphishing*" in the Evidence ID 10 in Table 4 while revealed the following identities:
    a. gonnagetphished@gmail.com was IDed as **Mr. Ronald Brown**
    b. phlatoutphishing@yahoo.com.au was IDed as **Mr. Justin Case**

    The ID was determined based on examining the text contents of the email sent to Mr. Brown by Mr. Case who had set up the phishing website. The names appeared immediately before the IDs listed on the text which indicates that this information was stored in Yahoo contact list on the Yahoo server.

35. Mr. Justin Case tells the suspect that the phishing website is designed to capture the user's account and password details before redirecting to the original bank website. This evidence is presented in Evidence ID 10 by searching for the search string "*password*".
36. Based on this information, the investigator further analysed the strings output file and observed that Mr. Ronald Brown's bank account information could have been phished by the website. The **account number 408854893** and **account password 96Cam** were retrieved from the strings output file. This could potentially incriminate the suspect and Mr. Justin Case if it can be verified that these are indeed account holder's bank information. Evidence is presented in Evidence ID 10 searching for the search string "*password*" which revealed the data:
    `action=validate&userid=408854893&password=96Cam&loginButton=Login`
37. Using the networking filters used internally by pyFLAG ver0.86RC1, the investigator browsed to the entire chat sessions which clearly indicate the intent to phish the said bank's website. Evidence ID 11 in Table 4 is presented in evidence. Chat stream contents contained in Evidence ID 26 – 37 in Table 4 support this claim.
38. The suspect has searched for and obtained a copy of WGET.exe which is a malware detection tool downloaded from http://users.ugent.be/~bpuype/wget. While this activity is not illegal, it becomes suspicious under the context of phishing activities reported during analysis. Evidence ID 14 and 15 listing the HTTP requests and responses from and to the suspect IP 192.168.1.103 is provided in support of this argument. Evidence ID 12 supports this claim.
39. The suspect has logged into the NAB website and spent considerable time downloading data. This is inferred from the HTTP packet contents in the transaction. Based on the analysis, it appears that the suspect attempted to mirror the website on to the local machine. Evidence ID 14 and 15 listing the HTTP requests and responses from and to the suspect IP 192.168.1.103 is provided in support of this argument.
40. The suspect has visited the IPRIMUS website. This could indicate that the suspect intended to obtain a connection with the ISP or probably already had a connection. Evidence ID 14 and 15 listing the HTTP requests and responses from and to the suspect IP 192.168.1.103 is provided in support of this argument. Evidence ID 12 supports this claim.

©Secure Cyber Space 2012

5. Supporting Evidence Presented

Evidence Identifier	Content	Content Source	Filename	MD5 HASH SUM
1	List of Ethernet endpoints	Wireshark ver0.99.7	Ethernet-endpoints.xml	eea937c53b56eb96ee486e9791f0ff1a
2	List of Ethernet conversations	Wireshark ver0.99.7	Ethernet-conversations.xml	b53e021a646a101528effd3f421f5b72
3	Packet contents of ARP	Wireshark ver0.99.7	arp-packet-displayed.txt	789608c5e84e821f318d33bf6e134182
4	List of IPv4 endpoints	Wireshark ver0.99.7	IPv4-endpoints.xml	f635897664b394ad4af4360a66254c68
5	List of IPv4 conversations	Wireshark ver0.99.7	IPv4-conversations.xml	df45c6db52730d5e12a7c0aefece459d
6	List of TCP endpoints	Wireshark ver0.99.7	TCP-endpoints.xml	ca8f1b7fd171591c93408e6d15b793ac
7	List of TCP conversations	Wireshark ver0.99.7	TCP-conversations.xml	039c0e2d86966faece8e0ccf76f06dda
8	List of UDP endpoints	Wireshark ver0.99.7	UDP-endpoints.xml	345939a014052e790011211f7e9f0efd
9	List of UDP conversations	Wireshark ver0.99.7	UDP-conversations.xml	00033f3948222b43a015d11ea268b41e
10	Strings output on PCAP file	‘strings’ on Linux	strings-output.txt	0eb8d6cafc89a811a6e4f26b7b6483d9
11	Messenger Chat session	pyFLAG ver0.86RC1	chat-session.xml	2ccf422b2ad9d72e8cd769945adb4460
12	HTTP session	pyFLAG ver0.86RC1	http-session.xml	9355b648a802ba093c88e7598362e5f8
13	CSV – XML conversion website list	Internet	Conversion-website.txt	33d01211c0864e44a69e95c9cb2a8113
14	Packet contents of all HTTP requests from suspect	Wireshark ver0.99.7	ipsrc-1921681103-http-req-compressed.txt	9c3a6bc4a46b0c582ec9a87242074f61
15	Packet contents of all HTTP responses to suspect	Wireshark ver0.99.7	ipdst-1921681103-http-resp-compressed.txt	d7445ef44c4f265817dbe05156082038
16	Packet contents of MSN messenger traffic from suspect	Wireshark ver0.99.7	ipsrc-1921681103-msnms-compressed.txt	1a99ac4213783c41786d2b01481fdc9a
17	Packet contents of MSN messenger traffic to suspect	Wireshark ver0.99.7	ipdst-1921681103-msnms-compressed.txt	0ef1bc04229cd2223c09855aa69dfe26
18	Packet contents of DNS queries to Router	Wireshark ver0.99.7	ipdst-19216811-dns-query-compressed.txt	7d8047afdddb413ceee30c04172d1302
19	Packet contents of DNS responses from Router	Wireshark ver0.99.7	ipsrc-19216811-dns-resp-	6dcb1f190c69ddb0bb16d1cab6c327c5

©Secure Cyber Space 2012

			compressed.txt	
20	Packet contents of TCP traffic from Router	Wireshark ver0.99.7	ipsrc-19216811-tcp-req-compressed.txt	f6bdf4e7ac0c24af91c1f4639ecde1b1
21	Packet contents of TCP traffic to Router	Wireshark ver0.99.7	ipdst-19216811-tcp-resp-compressed.txt	43885819273489c10f8a1a9589d04418
22	Load analysis on PCAP file	Wireshark ver0.99.7	graphanalysis.txt	e36791efd10a546ac05837cb4f8b3bbb
23	Load analysis on PCAP file with HTTP filter	Wireshark ver0.99.7	http-graphanalysis.txt	7fdf9fe496f39ef14c3a94832addb89b
24	Load analysis on PCAP file with MSNMS filter	Wireshark ver0.99.7	msnms-graphanalysis.txt	a2d6afff9e4524deefc1a1916718bc77
25	Streams and packet numbers map	pyFLAG ver0.86RC1	Mynotes.txt	facbe03b464cd5c56db4434757cbbf84
26	Packet contents of stream S133	pyFLAG ver0.86RC1	S133.txt	51a2af8bbde05c22a90772337196bb2f
27	Packet contents of stream S134	pyFLAG ver0.86RC1	S134.txt	8e43a0be6ad22d586ac7db26070cb15a
28	Packet contents of stream S170	pyFLAG ver0.86RC1	S170.txt	6b5a46d80285e890fafcf8bfa69dde8c
29	Packet contents of stream S171	pyFLAG ver0.86RC1	S171.txt	8ac46f011244a2d46fcd51a19780667b
30	Packet contents of stream S232	pyFLAG ver0.86RC1	S232.txt	eff476a4cd84a99e10e4af3805b19d60
31	Packet contents of stream S233	pyFLAG ver0.86RC1	S233.txt	c3931bf4b5b1434014a621bc858fbdb1
32	Packet contents of stream S331	pyFLAG ver0.86RC1	S331.txt	82fc890c10252f5a86b29455cac0b0b3
33	Packet contents of stream S332	pyFLAG ver0.86RC1	S332.txt	c28a23396e8ce5c58eca53be6dc8d43e
34	Packet contents of stream S362	pyFLAG ver0.86RC1	S362.txt	9c8451a41b50b274101f401e81a90ab7
35	Packet contents of stream S713	pyFLAG ver0.86RC1	S713.txt	bedc0feb5f99d73e26600263f70b5560
36	Packet contents of stream S716	pyFLAG ver0.86RC1	S716.txt	d4dab25e7b8c78348baf29186d489842
37	Packet contents of stream S1106	pyFLAG ver0.86RC1	S1106.txt	42f4e22fec06db5ac4409292d235ea86

Table 4. Tabulated list of evidence supporting the Forensic report

6. Conclusions

This report concludes that the suspect (IP 192.168.1.103) was planning to mirror the National Australia bank website along Mr. Justin Case (Yahoo ID: phlatoutphishing@yahoo.com.au). While it was Mr. Justin Case who hosted the phishing website, the report suspects that the aforementioned individuals have a track record for performing such illegal activities in the

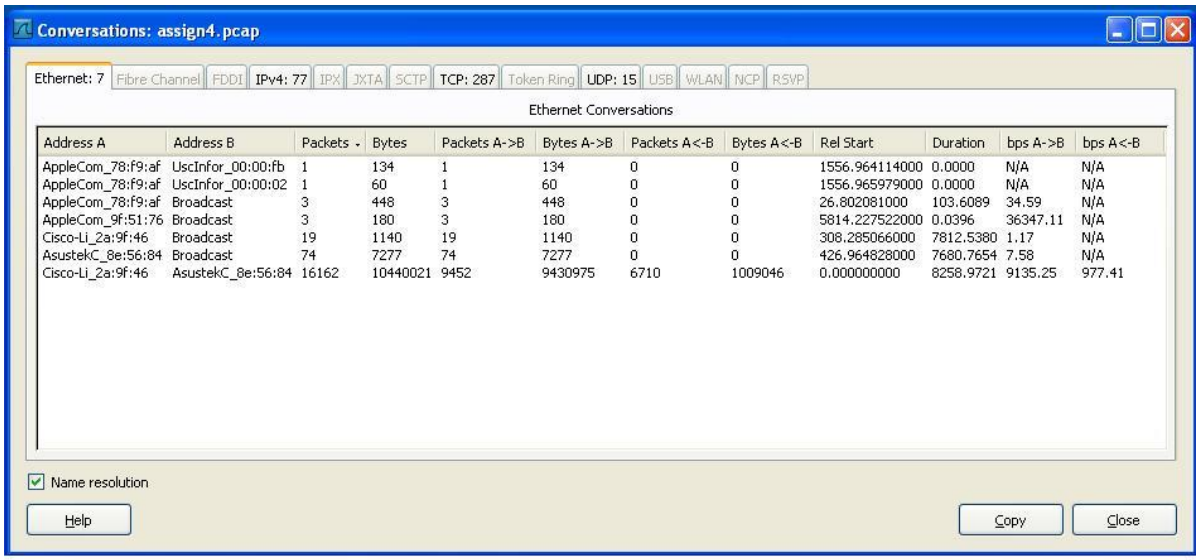
©Secure Cyber Space 2012

past. The report also believes that the suspect may have a first name/ middle name/ last name as Lamont detected from the machine name LAMONT01 from the NetBIOS datagram. The forensic analysis revealed that the suspect performed chat sessions with Mr. Justin Case using MSN ID lam3rallround@hotmail.com. Further, the suspect and his partner Mr. Justin Case have got together to plan and send out a phishing email to Mr. Ronald Brown with Google Mail ID gonnagetphished@gmail.com. According to the Australian Law HB-171, phishing is a punishable offence and there is sufficient evidence to track and arrest the suspect for further questioning. One should begin examining all public IP addresses within Australia under the subnet 192.168.1.xx and identify the actual subnet that was active during that period on 08th OCT 2006. This may be determined by checking past router logs (on the said date) at strategic points in Australia where the traffic bunches up. Based on the potential damage such activities can create, it is advisable to request Yahoo Australia to monitor the activities of the Mr. Justin Case with Yahoo ID phlatoutphishing@yahoo.com.au to come up with a location match. When a match is found, Mr. Justin Case may be arrested on charges of phishing and brought in for further questioning, possibly regarding similar activities in the past.

©Secure Cyber Space 2012

7. Appendix A – List of figures

Evidence 038



Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
AppleCom_78:f9:af	UscInfor_00:00:fb	1	134	1	134	0	0	1556.964114000	0.0000	N/A	N/A
AppleCom_78:f9:af	UscInfor_00:00:02	1	60	1	60	0	0	1556.965979000	0.0000	N/A	N/A
AppleCom_78:f9:af	Broadcast	3	448	3	448	0	0	26.802081000	103.6089	34.59	N/A
AppleCom_9f:51:76	Broadcast	3	180	3	180	0	0	5814.227522000	0.0396	36347.11	N/A
Cisco-Li_2a:9f:46	Broadcast	19	1140	19	1140	0	0	308.285066000	7812.5380	1.17	N/A
AsustekC_8e:56:84	Broadcast	74	7277	74	7277	0	0	426.964828000	7680.7654	7.58	N/A
Cisco-Li_2a:9f:46	AsustekC_8e:56:84	16162	10440021	9452	9430975	6710	1009046	0.000000000	8258.9721	9135.25	977.41

Description: Conversations tab under Statistics listing all Ethernet components detected on the Network. This was obtained using Wireshark ver0.99.7. The figure lists 6 distinct Ethernet components of which two devices with MAC addresses UscInfor-00-00-02 and UscInfor-00-00-FB were not active. The most active device on the network was device with MAC address AsustekC-8E-56-84 followed by Cisco-Li-2A-9F-46.

©Secure Cyber Space 2012

Evidence 039

Conversations: assign4.pcap

Ethernet: 7 | Fibre Channel | FDDI | IPv4: 77 | IPX | JXTA | SCTP | TCP: 287 | Token Ring | UDP: 15 | USB | WLAN | NCP | RSVP

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
192.168.1.1	192.168.1.103	442	110907	231	87011	211	23896	0.000000000	8183.3804	85.06	23.36
192.87.106.226	192.168.1.103	28	16193	16	15082	12	1111	527.041353000	12.3683	9755.28	718.61
165.228.133.11	192.168.1.103	397	226135	182	39762	215	186373	1256.040156000	5124.2188	62.08	290.97
157.193.40.15	192.168.1.103	476	388215	305	375543	171	12672	140.204757000	39.0999	76837.56	2592.74
125.252.194.70	192.168.1.103	10	1257	4	763	6	494	260.497186000	68.6565	88.91	57.56
125.7.34.123	192.168.1.103	114	92538	72	88160	42	4378	7639.945389000	582.3088	1211.18	60.15
68.142.236.11	192.168.1.103	287	180874	155	152291	132	28583	6597.408979000	1584.9444	768.69	144.27
68.142.213.132	192.168.1.103	481	107604	219	32836	262	74768	6570.882243000	1613.9250	162.76	370.61
66.102.7.147	192.168.1.103	12	2931	7	2157	5	774	1138.016310000	195.3294	88.34	31.70
66.102.7.104	192.168.1.103	11	1577	6	785	5	792	1137.598913000	193.9094	32.39	32.68
66.102.7.99	192.168.1.103	167	86890	98	71835	69	15055	0.090466000	343.0381	1675.27	351.10
66.94.234.13	192.168.1.103	9	1732	4	637	5	1095	6596.353208000	0.5547	9186.78	15792.04
66.94.230.23	192.168.1.103	11	3433	5	2244	6	1189	6878.039877000	0.6086	29498.90	15630.21
66.35.250.203	192.168.1.103	12	3646	6	2689	6	957	63.994630000	10.1364	2122.26	755.30
65.54.239.140	192.168.1.103	13	1153	6	603	7	550	242.067923000	0.9078	5314.13	4847.05
65.54.228.57	192.168.1.103	142	17333	70	8106	72	9227	6199.915297000	414.6183	156.40	178.03
65.54.228.31	192.168.1.103	30	3189	14	1597	16	1592	7075.815655000	100.9336	126.58	126.18
65.54.183.202	192.168.1.103	46	20073	22	12285	24	7788	242.008933000	2.9209	33647.26	21330.47
64.233.167.111	192.168.1.103	118	13454	65	8632	53	4822	2758.067360000	4202.9036	16.43	9.18
64.233.167.109	192.168.1.103	143	16549	77	10535	66	6014	358.133327000	6002.8086	14.04	8.01
64.233.163.111	192.168.1.103	85	9876	46	6300	39	3576	958.106063000	6602.6164	7.63	4.33
64.233.163.109	192.168.1.103	58	6667	32	4283	26	2384	5758.038031000	2403.0004	14.26	7.94
64.4.12.201	192.168.1.103	7	334	1	62	6	272	252.392655000	8.0852	N/A	269.13
64.4.12.200	192.168.1.103	8	496	1	62	7	434	247.366266000	9.6515	N/A	359.74
63.245.209.31	192.168.1.103	21	6318	10	4914	11	1404	179.841169000	0.9852	39903.17	11400.90
32.114.14.11	192.168.1.103	150	103638	84	96792	66	6846	1736.564920000	5476.3504	141.40	10.00
12.129.210.46	192.168.1.103	47	23752	19	13430	28	10322	6890.081727000	1311.4910	81.92	62.96
12.129.210.41	192.168.1.103	7	2105	3	1151	4	954	7566.091831000	23.4023	393.47	326.12
12.120.45.14	192.168.1.103	28	12044	12	9978	16	2066	3303.129323000	3909.6880	20.42	4.23
192.168.1.103	192.168.1.255	20	5009	20	5009	0	0	426.964828000	7573.5068	5.29	N/A
192.168.1.103	198.142.23.15	224	137924	102	19605	122	118319	6568.718905000	1690.2500	92.79	560.01
192.168.1.103	198.142.23.16	112	90100	43	6491	69	83609	8172.422984000	86.5374	600.06	7729.28
192.168.1.103	198.142.23.22	238	155112	106	27638	132	127474	6567.866170000	344.6876	641.46	2958.60
192.168.1.103	198.142.23.25	144	111336	56	6920	88	104416	6570.607204000	341.9493	161.90	2442.84
192.168.1.103	198.142.23.55	150	56748	78	26555	72	30193	6595.234526000	602.4039	352.65	400.97
192.168.1.103	198.142.23.62	65	37892	28	3451	37	34441	8107.096848000	151.8753	181.78	1814.17
192.168.1.103	198.142.23.63	17	6237	9	1519	8	4718	8105.988675000	152.9793	79.44	246.73
192.168.1.103	198.142.23.65	63	21154	27	5471	36	15683	6574.494359000	308.2360	142.00	407.04
192.168.1.103	198.142.23.70	164	114015	69	8556	95	105459	6568.847797000	1690.1171	40.50	499.18
192.168.1.103	198.142.23.71	1559	1340532	555	38130	1004	1302402	6889.879442000	307.7633	991.15	33854.64
192.168.1.103	198.142.23.78	11	2718	6	878	5	1840	8113.187838000	145.7799	48.18	100.97
192.168.1.103	198.142.23.80	16	6925	8	889	8	6036	6600.350795000	312.2192	22.78	154.66
192.168.1.103	198.142.23.81	50	9981	27	5979	23	4002	247.009757000	8000.2455	5.98	4.00
192.168.1.103	199.106.212.28	36	17772	20	2893	16	14879	1738.640506000	3673.6671	6.30	32.40
192.168.1.103	199.232.41.5	11	1478	6	702	5	776	105.746766000	73.4812	76.43	84.48
192.168.1.103	199.232.41.7	35	11879	18	3321	17	8558	119.495701000	29.7156	894.08	2303.97
192.168.1.103	199.232.41.10	98	43060	48	5966	50	37094	73.858522000	60.3570	790.76	4916.61
192.168.1.103	200.88.223.98	196	71182	82	45689	114	25493	7290.095636000	66.9502	5459.46	3046.20
192.168.1.103	203.16.234.90	5348	4725057	1819	99250	3529	4625807	528.244170000	40.8693	19427.76	905481.91
192.168.1.103	203.16.234.91	10	1305	6	729	4	576	528.124779000	10.9927	530.54	419.19
192.168.1.103	203.57.240.101	659	446481	269	46115	390	400366	1433.347835000	1106.7430	333.34	2894.01
192.168.1.103	203.57.241.101	725	470223	292	39842	433	430381	1659.899311000	5792.8167	55.02	594.37
192.168.1.103	203.57.241.103	755	497652	305	64102	450	433550	1475.060610000	6052.6525	84.73	573.04

Description: Conversations tab under Statistics listing all IP addresses detected on the Network. This was obtained using Wireshark ver0.99.7. Multiple IPs were detected of which 4 belong to the network that was monitored under the 192.168.1.xx subnet. Major portion of the remaining IPs belonged to external domains such as Google, Yahoo, MSN, etc. The most active IP was 192.168.1.103 which was determined as the suspect IP and this is associated with MAC address AsusTekC-8E-56-84.

©Secure Cyber Space 2012

Evidence 040

Conversations: assign4.pcap

Ethernet: 7 | Fibre Channel | FDDI | IPv4: 77 | IPX | JXTA | SCTP | TCP: 287 | Token Ring | UDP: 15 | USB | WLAN | NCP | RSVP

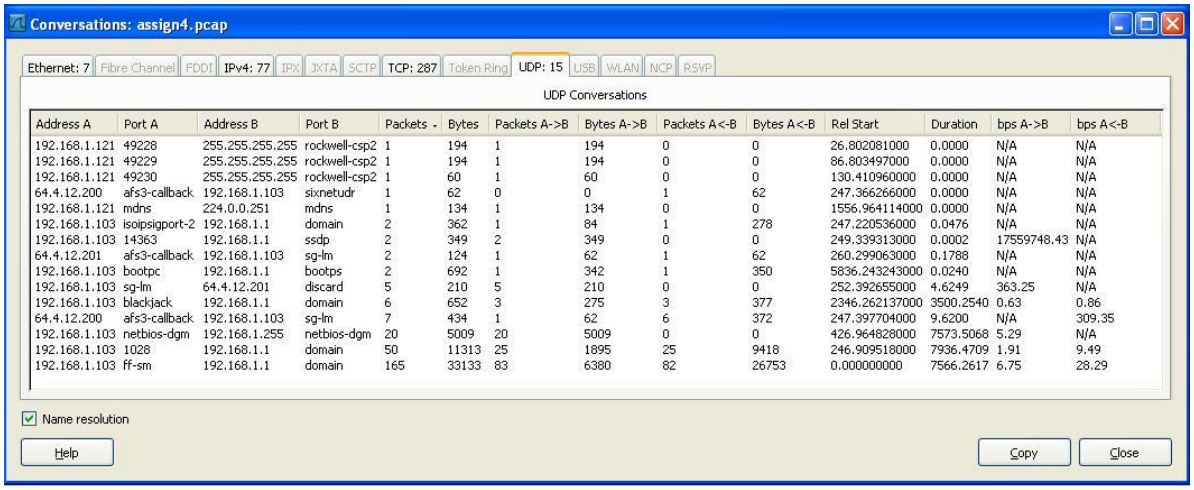
TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
192.168.1.103	netview-aix-8	203.16.234.90	http	5335	4720761	1812	98380	3523	4622381	546.013510000	23.1000	34070.98	1600823.97
192.168.1.103	radius-acct	198.142.23.71	http	1398	1209824	494	29017	904	1180807	6890.903178000	306.7392	756.79	30796.38
192.168.1.103	sightline	157.193.40.15	http	427	367382	148	9316	279	358066	144.740069000	34.5625	2156.33	82879.65
192.168.1.103	asi	203.57.241.103	https	324	245406	123	19141	201	226265	7475.218598000	22.5012	6805.32	80445.42
192.168.1.103	es-elmd	203.57.241.101	http	197	158912	71	5647	126	153265	7432.730237000	19.9855	2260.44	61350.42
192.168.1.103	deskshare	203.57.240.101	http	205	145368	84	8166	121	137202	2537.969859000	2.1210	30801.09	517508.08
192.168.1.103	scientia-sdb	198.142.23.71	http	161	130708	61	9113	100	121595	6889.879442000	307.7633	236.88	3160.74
192.168.1.103	swiftnet	198.142.23.25	http	144	111336	56	6920	88	104416	6570.607204000	341.9493	161.90	2442.84
192.168.1.103	ardt	203.57.241.103	https	165	114009	67	18090	98	95919	7474.654120000	1.9007	76139.93	403718.40
165.228.133.11	56815	192.168.1.103	31337	148	104321	58	13023	90	91298	6309.153106000	17.2315	6046.13	42386.53
192.168.1.103	3Com-nsd	198.142.23.22	http	148	102595	63	14329	85	88266	6567.866170000	344.6876	332.57	2048.60
192.168.1.103	mc2studios	198.142.23.16	http	112	90100	43	6491	69	83609	8172.422984000	86.5374	600.06	7729.28
192.168.1.103	ng-umds	203.57.240.101	http	123	92071	48	8929	75	83142	1473.161876000	22.9048	3118.65	29039.21
192.168.1.103	nsjtp-data	203.57.240.101	http	129	88447	54	10506	75	77941	1433.533363000	32.3955	2594.44	19247.39
192.168.1.103	rsvp-encap-1	203.57.241.101	http	121	78752	51	6905	70	71847	1660.397083000	2.3912	23101.34	240371.06
192.168.1.103	ftrapid-1	198.142.23.15	http	104	73284	43	7381	61	65903	6568.718905000	343.8435	171.73	1533.33
192.168.1.103	nsjtp-ctrl	203.57.240.101	http	110	73346	44	9630	66	63716	1433.347835000	32.5851	2364.27	15642.98
192.168.1.103	alpha-sms	210.50.7.243	http	73	58845	27	1948	46	56897	8106.443874000	0.4516	34508.57	1007922.98
192.168.1.103	street-stream	203.57.241.101	http	86	60213	33	4087	53	56126	6158.879175000	18.4539	1771.76	24331.30
192.168.1.103	oracle-em1	198.142.23.70	http	78	57940	31	3479	47	54461	6568.847797000	328.6950	84.67	1325.51
192.168.1.103	aspen-services	198.142.23.70	http	73	53788	30	3482	43	50306	6569.160922000	343.3862	81.12	1172.00
192.168.1.103	metrics-pas	203.57.241.101	https	78	50797	31	4552	47	46245	7433.609060000	19.0935	1907.24	19376.22
192.168.1.103	netopia-vo3	125.7.34.123	http	59	47359	22	2350	37	45009	7639.945389000	129.2331	145.47	2786.22
192.168.1.103	ftrapid-2	198.142.23.15	http	77	51385	33	6483	44	44902	6568.719597000	328.8632	157.71	1092.30
192.168.1.103	vids-avtp	210.50.7.243	http	56	44990	21	1615	35	43375	8107.006129000	0.7737	16698.85	448490.77
192.168.1.103	elm-momentum	125.7.34.123	http	55	45179	20	2028	35	43151	8183.386565000	38.8676	417.42	8881.63
192.168.1.103	rrirtr	203.57.241.103	https	84	51623	36	10451	48	41172	1475.060610000	20.9965	3981.99	15687.17
192.168.1.103	cinegrfx-lm	198.142.23.22	http	90	52517	43	13309	47	39208	6568.135784000	344.4058	309.15	910.74
192.168.1.103	itm-mcell-u	203.57.241.103	https	75	46198	32	7297	43	38901	7476.512338000	21.2148	2751.66	14669.35
192.168.1.103	rsvp-encap-2	32.114.14.11	http	57	41240	24	2604	33	38636	1736.564920000	494.8676	42.10	624.59
192.168.1.103	cisco-net-mgmt	203.84.217.32	http	44	33175	17	1444	27	31731	6567.642201000	0.2844	40614.85	892485.97
192.168.1.103	cft-2	203.84.217.32	http	42	33279	16	1661	26	31618	6592.638841000	0.3038	43734.41	832507.22
192.168.1.103	donnyworld	203.57.241.101	http	60	35200	26	5674	34	29526	7428.863465000	23.8525	1903.03	9902.84
192.168.1.103	empire-empuma	203.57.240.101	http	61	35975	26	6831	35	29144	1473.182087000	22.8849	2387.95	10188.05
192.168.1.103	lontalk-urgnt	66.102.7.99	http	59	33629	24	5579	35	28050	0.589311000	223.5585	199.64	1003.76
165.228.133.11	56777	192.168.1.103	31337	44	29567	17	1634	27	27933	6308.298480000	7.8282	1669.85	28545.87
192.168.1.103	direcpc-video	203.57.241.103	https	63	29565	25	3889	38	25676	7438.053159000	29.6591	1048.99	6925.63
192.168.1.103	rrifmm	203.57.241.101	http	42	26234	16	979	26	25255	1659.899311000	0.3119	25111.01	647782.11
192.168.1.103	visitview	216.52.244.214	http	36	26148	14	1292	22	24856	62.937521000	1.2073	8561.42	164707.99
192.168.1.103	unisys-lm	203.57.241.101	https	61	29627	26	5721	35	23906	7432.779261000	1.4654	31232.94	130511.21
207.46.108.16	msnp	192.168.1.103	shiva_confsrvr	598	47955	214	24467	384	23488	242.802817000	8004.6928	24.45	23.47
192.168.1.103	sunscalar-svc	198.142.23.62	http	38	23478	16	1834	22	21644	8107.365202000	151.6068	96.78	1142.11
165.228.133.11	59411	192.168.1.103	31337	42	26345	19	5978	23	20367	6371.819153000	8.0708	5925.58	20188.40
192.168.1.103	oraclenet8cman	66.102.7.99	http	42	23436	17	3313	25	20123	15.992102000	223.1675	118.76	721.36
192.168.1.103	canocentral1	210.50.7.243	http	31	21782	13	1832	18	19950	8112.194463000	0.3293	44504.23	484639.42
192.168.1.103	gsi	210.50.7.243	http	31	21699	13	1749	18	19950	8106.517024000	0.2883	48527.06	553524.73
192.168.1.103	islc	199.232.41.10	http	37	21297	17	1809	20	19488	103.869771000	30.3457	476.90	5137.59
192.168.1.103	slingshot	32.114.14.11	http	31	20807	14	1414	17	19393	3301.077412000	310.7882	36.40	499.20
192.168.1.103	rkb-oscs	32.114.14.11	http	31	20796	14	1414	17	19382	6905.692173000	307.2231	36.82	504.70
192.168.1.103	sesi-lm	32.114.14.11	http	31	20795	14	1414	17	19381	5103.435617000	308.9231	36.62	501.90
192.168.1.103	cft-7	198.142.23.55	http	74	30905	39	13660	35	17245	6595.234526000	602.4039	181.41	229.02
192.168.1.103	ncconfig	68.142.236.11	http	29	18536	13	2010	16	16526	8127.152976000	1.7872	8997.37	73975.43
192.168.1.103	tht-treasure	68.142.236.11	http	25	17340	11	1581	14	15759	7566.262776000	1.4342	8818.60	87901.48

Description: Conversations tab under Statistics listing all TCP components detected on the Network. This was obtained using Wireshark ver0.99.7. The analysis shows that there were several TCP transactions for the suspect IP 192.168.1.103 on port numbers > 5000 which indicates that the suspect visited custom websites. Based on the chat conversations, this report observes that the websites could be mirrored from standard websites to lure Internet browsers for phishing.

©Secure Cyber Space 2012

Evidence
041



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
192.168.1.121	49228	255.255.255.255	rockwell-csp2	1	194	1	194	0	0	26.802081000	0.0000	N/A	N/A
192.168.1.121	49229	255.255.255.255	rockwell-csp2	1	194	1	194	0	0	86.803497000	0.0000	N/A	N/A
192.168.1.121	49230	255.255.255.255	rockwell-csp2	1	60	1	60	0	0	130.410960000	0.0000	N/A	N/A
64.4.12.200	afs3-callback	192.168.1.103	sixnetudr	1	62	0	0	1	62	247.366266000	0.0000	N/A	N/A
192.168.1.121	mdns	224.0.0.251	mdns	1	134	1	134	0	0	1556.964114000	0.0000	N/A	N/A
192.168.1.103	isoipsigport-2	192.168.1.1	domain	2	362	1	84	1	278	247.220536000	0.0476	N/A	N/A
192.168.1.103	14363	192.168.1.1	ssdp	2	349	2	349	0	0	249.339313000	0.0002	17559748.43	N/A
64.4.12.201	afs3-callback	192.168.1.103	sg-lm	2	124	1	62	1	62	260.299063000	0.1788	N/A	N/A
192.168.1.103	bootpc	192.168.1.1	bootps	2	692	1	342	1	350	5836.243243000	0.0240	N/A	N/A
192.168.1.103	sg-lm	64.4.12.201	discard	5	210	5	210	0	0	252.392655000	4.6249	363.25	N/A
192.168.1.103	blackjack	192.168.1.1	domain	6	652	3	275	3	377	2346.262137000	3500.2540	0.63	0.86
64.4.12.200	afs3-callback	192.168.1.103	sg-lm	7	434	1	62	6	372	247.397704000	9.6200	N/A	309.35
192.168.1.103	netbios-dgm	192.168.1.255	netbios-dgm	20	5009	20	5009	0	0	426.964828000	7573.5068	5.29	N/A
192.168.1.103	1028	192.168.1.1	domain	50	11313	25	1895	25	9418	246.909518000	7936.4709	1.91	9.49
192.168.1.103	ff-sm	192.168.1.1	domain	165	33133	83	6380	82	26753	0.000000000	7566.2617	6.75	28.29

Description: Conversations tab under Statistics listing all UDP components detected on the Network. This was obtained using Wireshark ver0.99.7. Based on the transactions taking place in the UDP space, it appears to be mainly DNS request response pairs exchanged between 192.168.1.103 and 192.168.1.1 (Router). No suspicious traffic was observed.

©Secure Cyber Space 2012

Evidence 042

HTTP/Load Distribution with filter: http

Topic / Item	Count	Rate	Percent
www.google.com.au	13	0.000002	2.35%
htdig.binarycompass.org	3	0.000000	0.54%
sourceforge.net	1	0.000000	0.18%
www.gnu.org	5	0.000001	0.90%
directory.fsf.org	3	0.000000	0.54%
www.fsf.org	1	0.000000	0.18%
ftp.gnu.org	6	0.000001	1.08%
www.google.co.uk	8	0.000001	1.45%
users.ugent.be	8	0.000001	1.45%
login.live.com	1	0.000000	0.18%
c.msn.com	1	0.000000	0.18%
ak.imgag.com	17	0.000002	3.07%
rad.msn.com	7	0.000001	1.27%
239.255.255.250:1900	4	0.000000	0.72%
global.msads.net	1	0.000000	0.18%
fpdownload.macromedia.com	1	0.000000	0.18%
httpd.apache.org	1	0.000000	0.18%
planetmirror.com	1	0.000000	0.18%
public.planetmirror.com	1	0.000000	0.18%
apache.planetmirror.com.au	1	0.000000	0.18%
192.168.1.1	12	0.000001	2.17%
www.national.com.au	126	0.000015	22.78%
203.57.240.101	82	0.000010	65.08%
203.57.241.101	44	0.000005	34.92%
forecastfox.accuweather.com	5	0.000001	0.90%
sirocco.accuweather.com	5	0.000001	0.90%
www.yahoo.com.au	1	0.000000	0.18%
au.yahoo.com	6	0.000001	1.08%
l.yimg.com	56	0.000007	10.13%
198.142.23.22	52	0.000006	92.86%
198.142.23.62	4	0.000000	7.14%
au.biz.yahoo.com	1	0.000000	0.18%
ichart.yahoo.com	1	0.000000	0.18%
au.i1.yimg.com	24	0.000003	4.34%
au.a1.yimg.com	10	0.000001	1.81%
us.js2.yimg.com	11	0.000001	1.99%
row.bc.yahoo.com	48	0.000006	8.68%
68.142.213.132	48	0.000006	100.00%
au.srd.yahoo.com	3	0.000000	0.54%

Description: HTTP load distribution pattern with `http` filter on the Statistics tab listing all TCP components detected on the Network. This was obtained on the HTTP load distribution under Statistics tab using Wireshark ver0.99.7. The tool was enabled to perform name resolution on the network layer listed in the View tab under Name Resolution. The sequence of websites listed is approximate to the actual sequence as recovered from the analysis.

©Secure Cyber Space 2012

Evidence 043

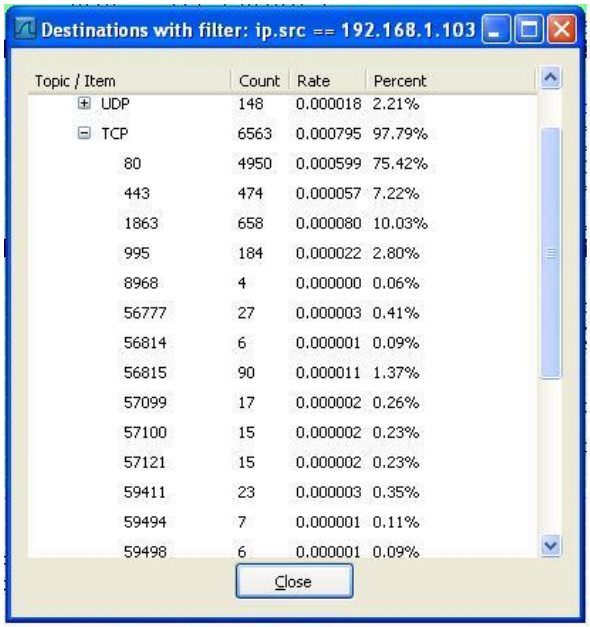
HTTP/Load Distribution with filter: ip.src == 192.168.1.103

Topic / Item	Count	Rate	Percent
HTTP Requests by Server	553	0.000068	
HTTP Requests by Server Address	553	0.000068	100.00%
HTTP Requests by HTTP Host	553	0.000068	100.00%
www.google.com	2	0.000000	0.36%
www.google.com.au	13	0.000002	2.35%
htdig.binarycompass.org	3	0.000000	0.54%
sourceforge.net	1	0.000000	0.18%
www.gnu.org	5	0.000001	0.90%
directory.fsf.org	3	0.000000	0.54%
www.fsf.org	1	0.000000	0.18%
ftp.gnu.org	6	0.000001	1.08%
www.google.co.uk	8	0.000001	1.45%
users.ugent.be	8	0.000001	1.45%
login.live.com	1	0.000000	0.18%
c.msn.com	1	0.000000	0.18%
ak.imgag.com	17	0.000002	3.07%
rad.msn.com	7	0.000001	1.27%
239.255.255.250:1900	4	0.000000	0.72%
global.msads.net	1	0.000000	0.18%
fpdownload.macromedia.com	1	0.000000	0.18%
httpd.apache.org	1	0.000000	0.18%
planetmirror.com	1	0.000000	0.18%
public.planetmirror.com	1	0.000000	0.18%
apache.planetmirror.com.au	1	0.000000	0.18%
192.168.1.1	12	0.000001	2.17%
www.national.com.au	126	0.000015	22.78%
203.57.240.101	82	0.000010	65.08%
203.57.241.101	44	0.000005	34.92%
forecastfox.accuweather.com	5	0.000001	0.90%
sirocco.accuweather.com	5	0.000001	0.90%
www.yahoo.com.au	1	0.000000	0.18%
au.yahoo.com	6	0.000001	1.08%
l.yimg.com	56	0.000007	10.13%
198.142.23.22	52	0.000006	92.86%
198.142.23.62	4	0.000000	7.14%
au.biz.yahoo.com	1	0.000000	0.18%
ichart.yahoo.com	1	0.000000	0.18%
au.i1.yimg.com	24	0.000003	4.34%

Description: HTTP load distribution pattern with `ip.src == 192.168.1.103` filter on the Statistics tab listing all TCP components detected on the Network. This was obtained on the "HTTP load distribution" under Statistics tab using Wireshark ver0.99.7. The tool was enabled to perform name resolution on the network layer listed in the View tab under Name Resolution. The sequence of websites listed is approximate to the actual sequence as recovered from the analysis.

©Secure Cyber Space 2012

Evidence 044



Topic / Item	Count	Rate	Percent
UDP	148	0.000018	2.21%
TCP	6563	0.000795	97.79%
80	4950	0.000599	75.42%
443	474	0.000057	7.22%
1863	658	0.000080	10.03%
995	184	0.000022	2.80%
8968	4	0.000000	0.06%
56777	27	0.000003	0.41%
56814	6	0.000001	0.09%
56815	90	0.000011	1.37%
57099	17	0.000002	0.26%
57100	15	0.000002	0.23%
57121	15	0.000002	0.23%
59411	23	0.000003	0.35%
59494	7	0.000001	0.11%
59498	6	0.000001	0.09%

Description: List of all TCP destinations with `ip.src == 192.168.1.103` filter on the Statistics tab listing all TCP components detected on the Network. This was obtained on the "Destinations" under Statistics tab using Wireshark ver0.99.7. This figure shows that the suspect predominantly maintained TCP transactions on the HTTP port. However, there are several ports with port numbers > 5000 listed. This leads to suspect the fact that the suspect hosted mirrored websites for phishing. The tool was enabled to perform name resolution on the network layer listed in the View tab under Name Resolution. The sequence of websites listed is approximate to the actual sequence as recovered from the analysis.

©Secure Cyber Space 2012