Network Forensics and its Scope & Role

kevinkoo001@gmail.com

May 2013

Overview

1. Introduction

2. Considerations

3. Scope & Role for Network Forensic (Discussion)

4. Packet Analysis for Network Forensics

Introduction

- **Network?**
  - Protocols
  - Devices
  - Packets never lie!

- **Methodology (OSCAR)**
  - Obtain information
  - Strategize
  - Collect Evidence
  - Analyze
  - Report

Considerations

- **What to know when an incident occurs over network**
  - Description
  - Date, time, and method of incident discovery
  - Persons involved
  - Systems and data involved
  - Actions taken since discovery
  - Summary of internal discussions
  - Incident manager and process
  - Legal issues
  - Time frame for investigation/recovery/resolution
  - Goals

Considerations

- **The properties (thus challenges) of Network-based digital evidence**
  - **Communication**: Between the two or among multiple participants at a certain point
  - **Volatile**: The matter of when, hard to find artifacts even in memory
  - **Scattered**: No choice but to get involved multiple sources of evidence
  - **Storage**: Possibly stores all packets on the fly??
  - **Privacy**: Problematic if storage is available depending on jurisdiction
  - **Seizure**: Seizing a network device with a warrant?
  - **Admissibility**: No file system and no standard format → admissible in court?
  - **Encryption**: Hard to identify network traffic even though it's detected.

Scope & Role for Network Forensic

- **Things taken into account**

  - Acquirements → Standard? Format? C.I.A?
  - Storage → Chain of Custody

    Who is eligible to get access to potential evidence?

    How can collected network evidence be handled in a forensically sound manner?
  - How to prove the originals and the copies
  - Analysis → Correlation from multiple sources of evidence

    Are all timestamp trustworthy?

    Is skewed timeline allowable to court?

    Extracted files over network!
  - Repeatable?

Scope & Role for Network Forensic

- **DISCUSSION: Then how much does network forensics cover?**

  - Network packet acquirement → mandatory?
  - If so, are all network range included? Both on the wire and in the air?? Cost???
  - Are the followings part of network forensics?

    Log analysis for correlation

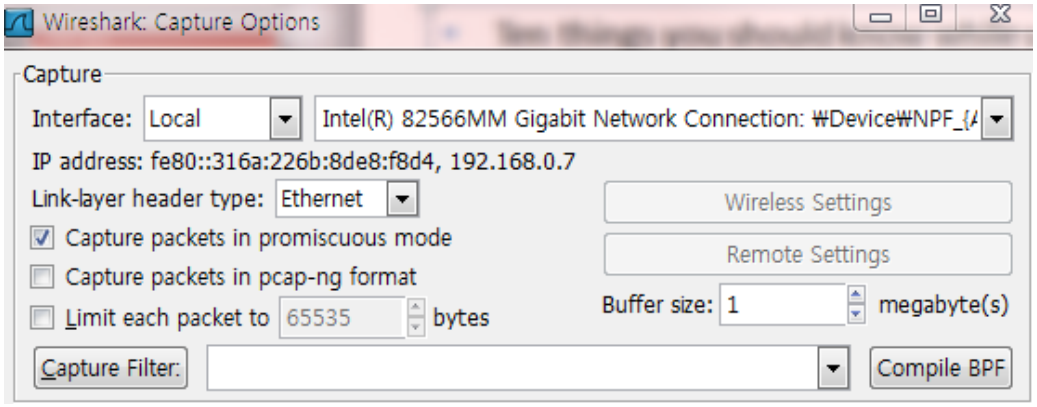
    Executable found in the packets

    Encrypted payloads in the packets (SSL/TLS/other home-brewed techniques, …)
  - If so, is the investigation from network-oriented security devices itself as well as all logs (eg. IDS, IPS, WAF, …)?
  - In real time or Post-investigation? Cost? Mandatory?
  - Putting all together, what should be defined as forensic readiness?

Packet Analysis for Network Forensics

▪ Tips to use *Wireshark* wisely (1/7)

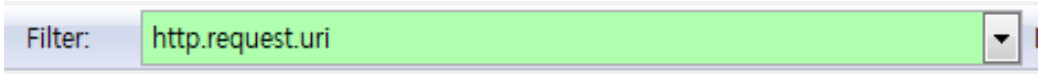
- Two different filters to help to investigate desired traffic (1)
  - ❖ **Traffic Capture Filter**
  - ❖ BNF (Berkeley Packet Filtering) in straightforward syntax (capture → capture options or Ctrl+K)



(1) host 192.168.0.25
(2) net 192.168.8.0/24 or net 192.168.8.0 mask 255.255.255.0
(3) src net 192.168.0.0/16 or net 192.168.0.0 mask 255.255.0.0
(4) port 53
(5) host www.example.com and not (port 80 or port 25)
(6) port not 53 and not arp
(7) tcp portrange 1000-2000

▪ Tips to use *Wireshark* wisely (2/7)

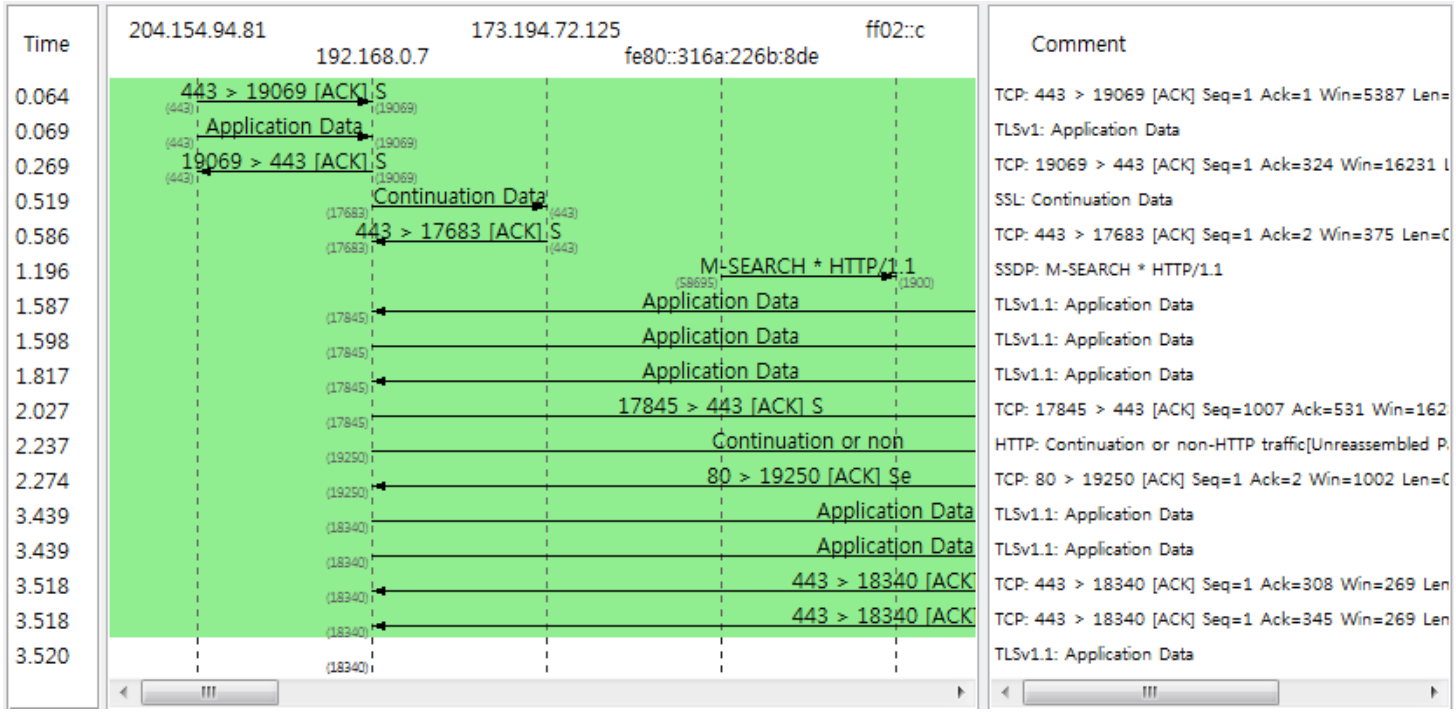
- Two different filters to help to investigate desired traffic (2)
  - ❖ **Display Filter** (http://www.wireshark.org/docs/dfref/)
  - ❖ Wireshark's own syntax



(1) tcp.port eq 25 or icmp
(2) ip.src == 192.168.8.0/24 and ip.dst == 192.168.0.0/16
(3) http || ssl
(4) eth.addr [0:3] == 00:06:5B
(5) udp contains 81:60:03
(6) http.request.uri
(7) ip.addr == 10.1.2.3
(8) ip.addr != 10.2.3.4 or ip.dst != 10.6.7.9
(9) !(ip.src == 10.11.12.13)

Tips to use *Wireshark* wisely (3/7)

- Flows of entire packets in details graphically!
  - Menu → Statistics → FlowGraph



- **Tips to use *Wireshark* wisely (4/7)**

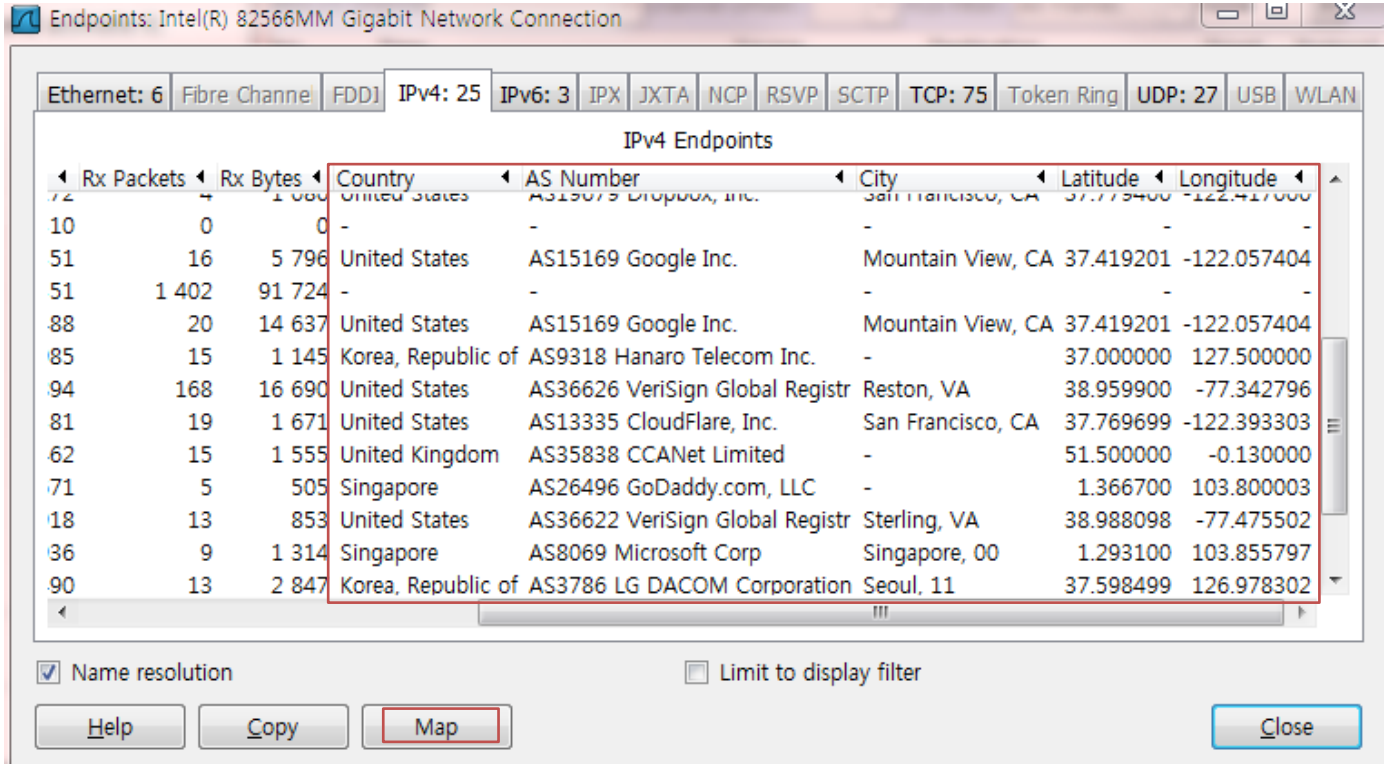
  - Statistics of entire packets in details graphically!

    - Menu → Statistics → I/O Graphs

- **Tips to use *Wireshark* wisely (5/7)**

  - How to identify location information with *GeoLocation* in real time!

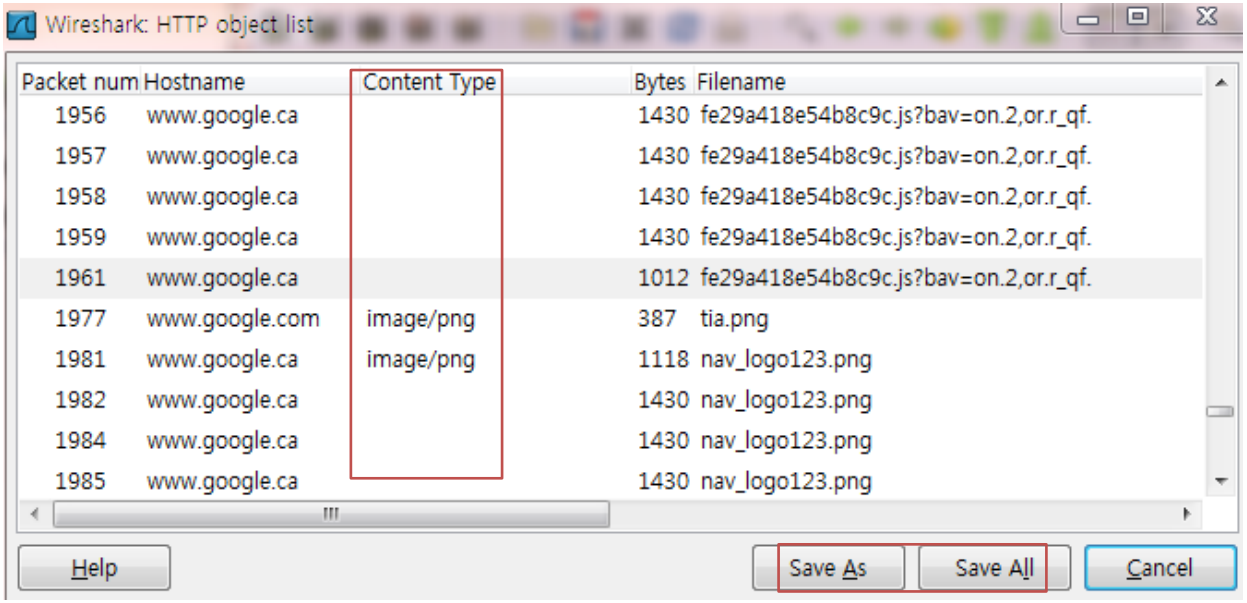
    - Download the *GeoIP* Location from *Maxmind* and activate it.
    - Menu → Statistics → Endpoints



- **Tips to use *Wireshark* wisely (6/7)**

  - How to Extract HTTP, SMB objects from what you have captured.

    - Menu → File → Export → Objects → {HTTP, SMB}



- **How to get abnormal packets quickly**
  - Expert Infos

- **Tips to use *Wireshark* wisely (7/7)**
  - Powerful command-line tools (https://www.wireshark.org/docs/man-pages/)
    - capinfos - Prints information about capture files
    - dftest - Shows display filter byte-code, for debugging dfilter routines.
    - dumpcap - Dump network traffic
    - editcap - Edit and/or translate the format of capture files
    - idl2wrs - CORBA IDL to Wireshark Plugin Generator
    - mergecap - Merges two or more capture files into one
    - randpkt - Random Packet Generator
    - rawshark - Dump and analyze raw libpcap data
    - text2pcap - Generate a capture file from an ASCII hexdump of packets
    - tshark - Dump and analyze network traffic
    - wireshark-filter - Wireshark filter syntax and reference
    - wireshark - Interactively dump and analyze network traffic

Getting used to abnormal network traffic with Samples

- **Trace files from *Wireshark.org***

  - 239 (1.87GB in size) pcap examples (http://wiresharkbook.com/studyguide.html)

    - ❖ Great samples to learn naïve network traffic
    - ❖ Try to catch the property of suspicious packets in particular, in advance

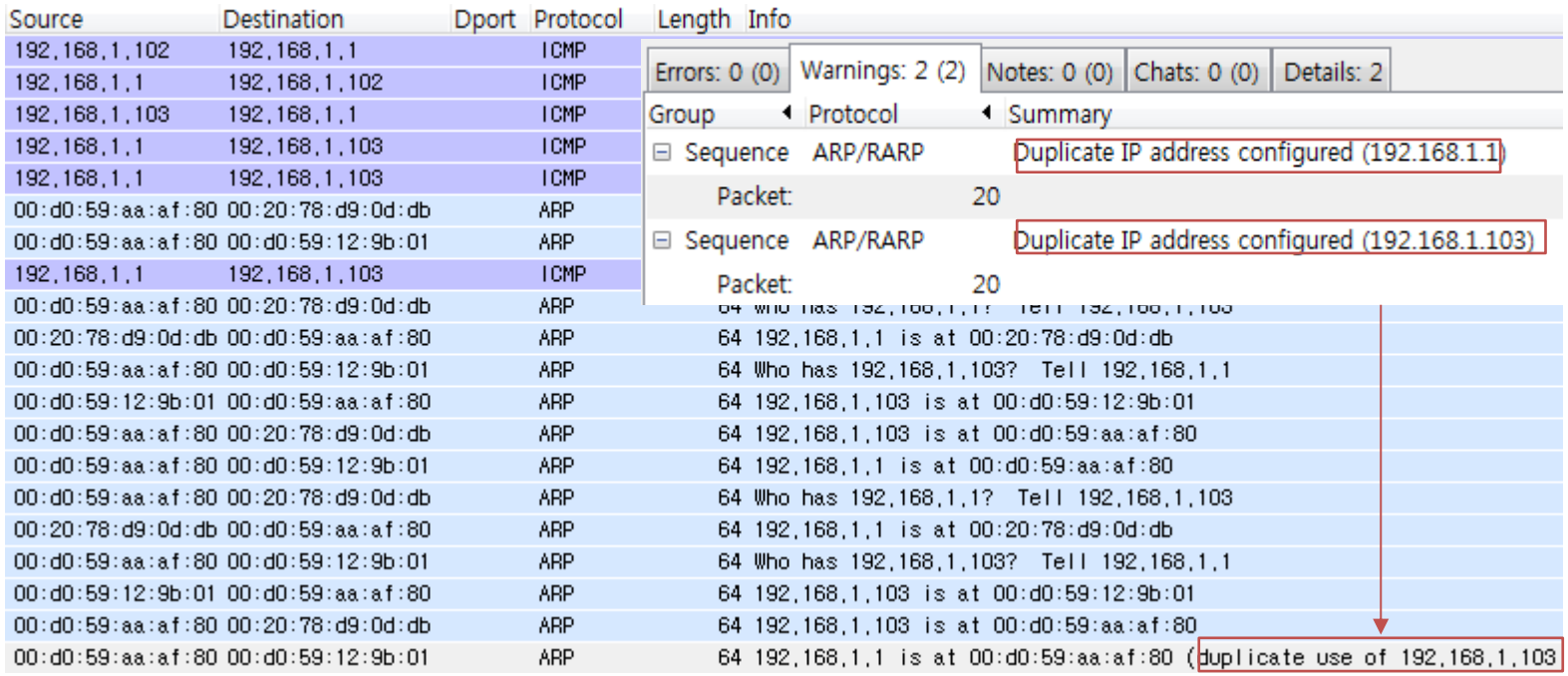
WIRESHARK BOOK

Book Supplements

- All supplements [1.5 GB]
- Wireshark Trace Files [1.5 GB]
- - Trace Files (Set 1) [324 MB]
- - Trace Files (Set 2) [212 MB]
- - Trace Files (Set 3) [504 MB]
- - Trace Files (Set 4) [504 MB]
- Wireshark Configs [122 KB]
- Chanalyzer Files [1.5 MB]
- GeoIP Databases [40.5 MB]
- PhoneFactor Files [612 KB]
- Jumpstart Videos (Link)

- **ARP Poisoning (*arp-poison.pcap*)**

  - Duplicate IP addresses are Detected!!



- **Dictionary Attack (*sec-dictionary2.pcap*)**

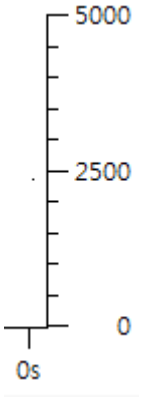
  - Dictionary attack against FTP server was performed!
  - Filter: "**ftp.request.command==PASS**"

Source	Destination	Dport	Protocol	Length	Info
69.181.135.56	67.161.39.46	21	FTP	61	Request: PASS
69.181.135.56	67.161.39.46	21	FTP	65	Request: PASS salt
69.181.135.56	67.161.39.46	21	FTP	64	Request: PASS aaa
69.181.135.56	67.161.39.46	21	FTP	64	Request: PASS abc
69.181.135.56	67.161.39.46	21	FTP	69	Request: PASS academia
69.181.135.56	67.161.39.46	21	FTP	69	Request: PASS academic
69.181.135.56	67.161.39.46	21	FTP	67	Request: PASS access
69.181.135.56	67.161.39.46	21	FTP	64	Request: PASS ada
69.181.135.56	67.161.39.46	21	FTP	66	Request: PASS admin
69.181.135.56	67.161.39.46	21	FTP	74	Request: PASS administrator
69.181.135.56	67.161.39.46	21	FTP	67	Request: PASS adrian
69.181.135.56	67.161.39.46	21	FTP	69	Request: PASS adrianna
69.181.135.56	67.161.39.46	21	FTP	69	Request: PASS aerobics
69.181.135.56	67.161.39.46	21	FTP	69	Request: PASS airplane
69.181.135.56	67.161.39.46	21	FTP	67	Request: PASS albany
69.181.135.56	67.161.39.46	21	FTP	70	Request: PASS albatross

Getting used to abnormal network traffic with Samples

- **MAC Flooding (*sec-macof.pcap*)**

  - I/O Graph shows too many packets had flooded over network! (1.28Mbps)
  - Source MAC must not be a group address. (Wireshark Expert Infos)



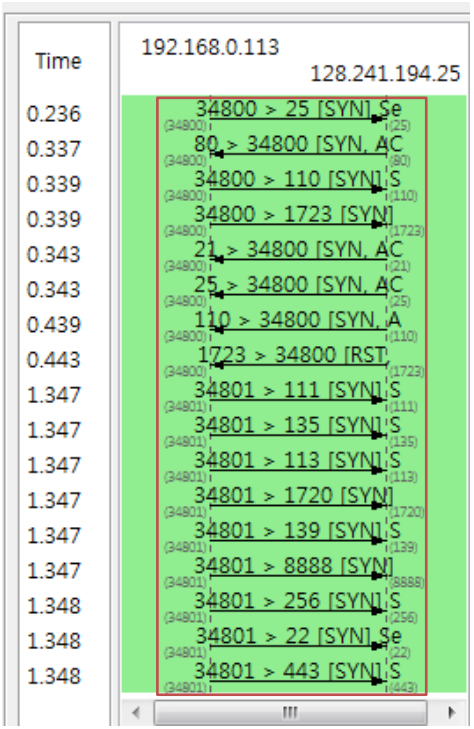
Source	Destination	Dport	Protocol	Length	Info
175,18,32,32	165,245,182,49	54165	TCP	54	38057 > 54165 [SYN] Seq=0 Win=512 Len=0
155,0,224,30	205,97,234,95	40175	TCP	54	8411 > 40175 [SYN] Seq=0 Win=512 Len=0
36,34,44,78	222,180,154,69	59230	TCP	54	9098 > 59230 [SYN] Seq=0 Win=512 Len=0
144,244,116,122	49,12,196,124	33710	TCP	54	4925 > 33710 [SYN] Seq=0 Win=512 Len=0
83,6,90,102	144,16,241,65	3464	TCP	54	31155 > 3464 [SYN] Seq=0 Win=512 Len=0
112,180,104,73	20,143,226,119	41314	TCP	54	54643 > 41314 [SYN] Seq=0 Win=512 Len=0
25,189,117,0	253,145,32,54	53451	TCP	54	747 > 53451 [SYN] Seq=0 Win=512 Len=0
20,249,144,0	43,241,39,65	29528	TCP	54	63694 > 29528 [SYN] Seq=0 Win=512 Len=0
247,159,79,92	211,69,124,125	20923	TCP	54	53696 > 20923 [SYN] Seq=0 Win=512 Len=0
47,72,73,58	149,104,191,102	34148	TCP	54	16060 > 34148 [SYN] Seq=0 Win=512 Len=0
154,139,26,46	83,58,134,11	45699	TCP	54	23762 > 45699 [SYN] Seq=0 Win=512 Len=0
14,45,16,11	122,194,198,119	2527	TCP	54	9097 > 2527 [SYN] Seq=0 Win=512 Len=0
87,119,201,40	156,106,154,40	57052	TCP	54	11024 > 57052 [SYN] Seq=0 Win=512 Len=0

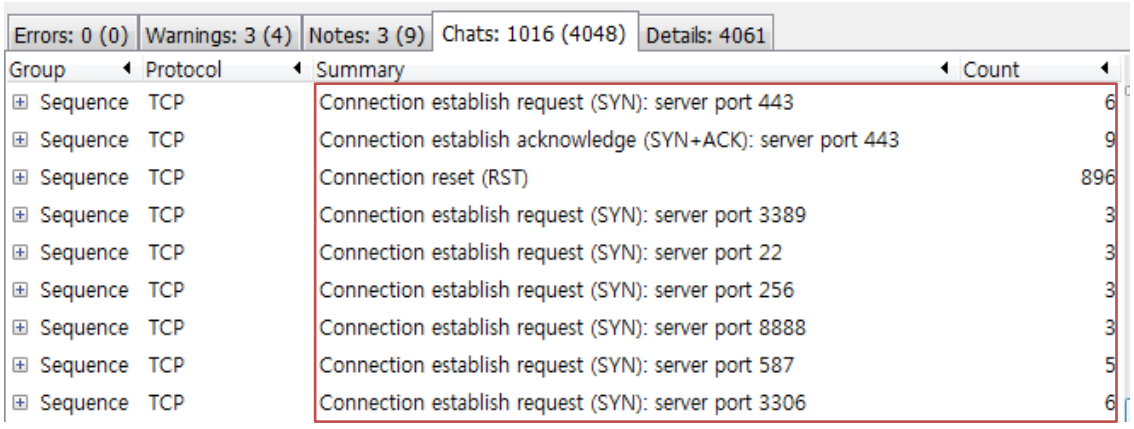
```
⊞ Frame 13341: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊟ Ethernet II, Src: f7:53:e0:39:8b:e9 (f7:53:e0:39:8b:e9), Dst: 8f:46:2b:16:6b:b9 (8f:46:2b
  ⊞ Destination: 8f:46:2b:16:6b:b9 (8f:46:2b:16:6b:b9)
  ⊟ Source: f7:53:e0:39:8b:e9 (f7:53:e0:39:8b:e9)
    ⊞ [Expert Info (Warn/Protocol): Source MAC must not be a group address: IEEE 802.3-200
      Address: f7:53:e0:39:8b:e9 (f7:53:e0:39:8b:e9)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT th
  Type: IP (0x0800)
```

Getting used to abnormal network traffic with Samples

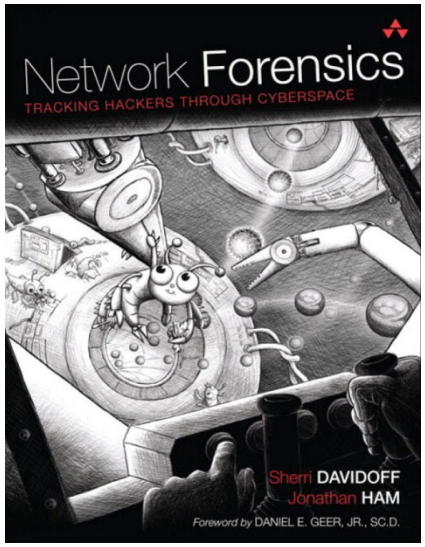
- **Port Scanning (*sec-nmap-osdetect-sV-O-v.pcap*)**

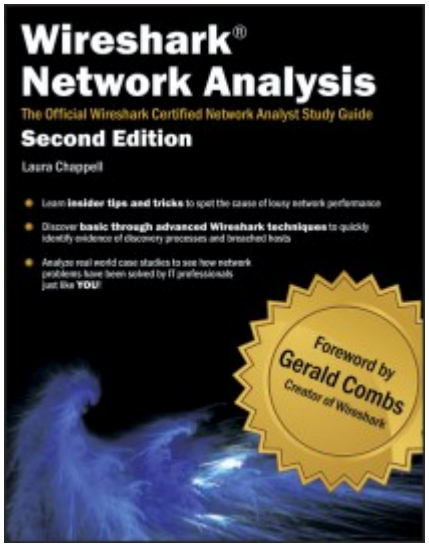
  - The same source IP, many destination ports in a target and/or many SYN/ACKs and FINs.





References


Network Forensics
TRACKING HACKERS THROUGH CYBERSPACE
Sherri DAVIDOFF
Jonathan HAM
Foreword by DANIEL E. GEER, JR., SC.D.


Wireshark®
Network Analysis
The Official Wireshark Certified Network Analyst Study Guide
Second Edition
Laura Chappell
Foreword by
Gerald Combs
Creator of Wireshark

Question and Answer