Lesson 8: Penetration Testing and Audits

Vulnerability Scan v Pen Test v Audit

Vulnerability Scan

Uses tools to scan for known vulnerabilities

Pen Test

Actually attempts to break into the network

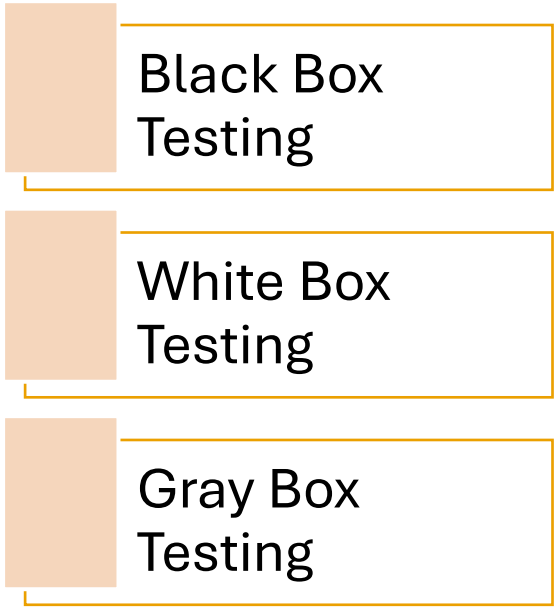
Audit

Checking logs, policies, looks for compliance to policies

Terminology

- **Ad hoc testing**: Testing carried out with no systematic approach or methodology. It is hoped that this book will steer you away from that.
- **Black hat hacker**: A hacker who does break the law. This term is synonymous with cracker, but the term *black hat hacker* is far more common. Contrary to some media portrayals, a black hat is not necessarily any more skilled. Someone can break the law and still have only minimal skill.
- **Cracker**: One who breaks into a system in order to do something malicious, illegal, or harmful. Synonymous with black hat hacker.
- **Ethical hacking**: Someone who is using hacking techniques for legal and ethical purposes.
- **Footprinting**: Scanning a target to learn about that target.
- **Gray hat hacker**: A hacker who usually obeys the law but in some instances will cross the line into black hat hacking.
- **Hacker**: One who tries to learn about a system by examining it in detail by reverse-engineering or probing the system. This is an important definition. Hackers, are not necessarily criminals. One can be a hacker and never break the law, nor do anything unethical.
- **Script kiddy**: A slang term for an unskilled person who purports to be a skilled hacker. Some people download a tool or two, learn to use those, then consider themselves great hackers, when they are not.
- **White hat hacker**: A hacker who does not break the law, often synonymous with ethical hacker. Essentially this is a person who uses hacking skills in a legal and ethical manner.

Testing Terms



Note: White box is also known as clear box testing, glass box testing, transparent box testing, and structural testing

Quality of Security Testing

Reasons for false negatives

The Tester

The Objectives

Test Coverage

NIST 800-115

NIST 800-115 describes security assessments and has four phases:

Planning

Discovery

Attack

Reporting

NIST 800-115

Image from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

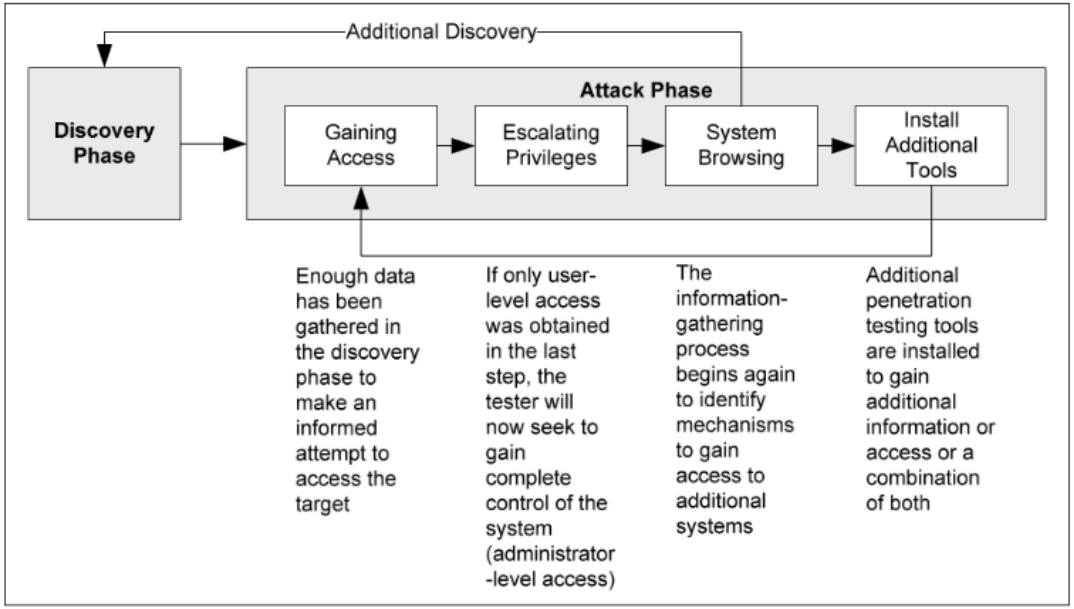


Figure 5-2. Attack Phase Steps with Loopback to Discovery Phase

NIST 800-115

Implement a repeatable and documented assessment methodology.

Determine the objectives of each security assessment, and tailor the approach accordingly.

Analyze findings, and develop risk mitigation techniques to address weaknesses.

NIST 800-115

Security Testing Technique	Security Testing Tool
Review	
Network Sniffing	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer, and Wireshark
File Integrity Checking	Autopsy, Foremost, RootkitHunter, and Sleuthkit
Target Identification and Analysis	
Application Security Testing	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, and Peach
Network Discovery	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, and Umit
Network Port and Service Identification	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, and UnicornScan
Vulnerability Scanning	Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Snort, and SuperScan
Wireless Scanning	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet, and WifiTAP
Target Vulnerability Validation	
Password Cracking	Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, and WebCrack
Remote Access Testing	IKEProbe, IKE-Scan, PSK-Crack, and VNC_bypauth
Penetration Testing	Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer, and Wireshark

Image from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

National Security Agency (NSA) Information Assessment Methodology (IAM)

Pre-Assessment

On-site

Post Assessment

NSA-IAM Overview

Pre-Assessment

Determine and manage the customer's expectations

Gain an understanding of the organization's information criticality

Determine customer's goals and objectives

Determine the system boundaries

Coordinate with customer

Request documentation

On-Site Assessment

Conduct opening meeting

Gather and validate system information (via interview, system demonstration, and document review)

Analyze assessment information

Develop initial recommendations

Present out-brief

Post-Assessment

Additional review of documentation

Additional expertise (get help understanding what you learned)

Report coordination (and writing)

See also http://www.isaca.org/Journal/archives/2007/Volume-2/Documents/jopdf0702-info-security-request.pdf

IAM

Information Criticality matrix

System Criticality matrices

Baseline INFOSEC evaluation areas

Technical Assessment Plan (TAP)

http://www.sans.org/reading-room/whitepapers/auditing/application-nsa-infosec-assessment-methodology-1045

http://systemexperts.com/media/pdf/NSAIAM.pdf

PCI Penetration Testing standard

Scope

Qualifications of a Penetration tester

Penetration Testing Components

Methodology

Pre-engagement

> Pre-engagement includes scoping, documentations (network diagram, cardholder data flow diagram, etc.), rules of engagement, success criteria, review of past issues.

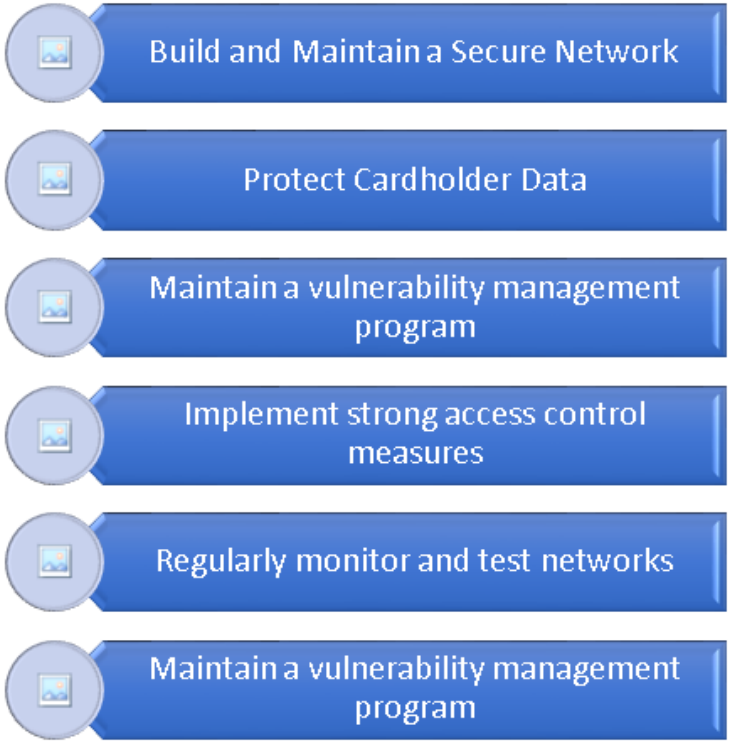
The actual penetration test

Post-Engagement

> Remediation best practices, retest vulnerabilities, reporting and documentation standards.

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PCI Penetration Testing standard



PCI Penetration Testing standard

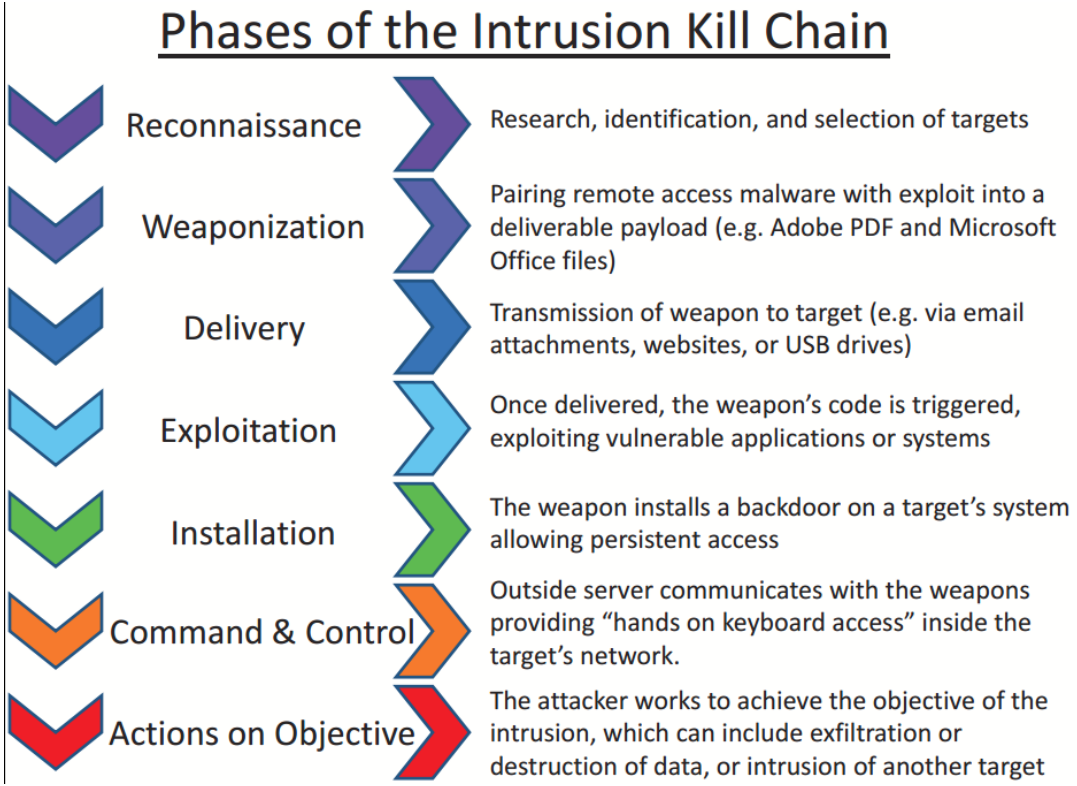
	Vulnerability Scan	Penetration Test
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly or after significant changes.	At least annually and upon significant changes. (Refer to Section 2.6 of this document for information on significant changes.)
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

Chart from Penetration Testing Guidance
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PCI Highlights

Pre-Engagement	Actual Test	Post-Engagement
• Scope • Documentation • Rules of engagement • Environment • Success Criteria • Past vulnerability scans	• Application Layer • Network Layer • Segmentation • How to handle card holder data • Post-exploitation	• Remediation • Retesting identified vulnerabilities • Cleaning Up • Reporting

Cyber Kill Chain



CEH Lifecycle

Gain Access

Escalate Privileges

Execute Applications

Hide Files

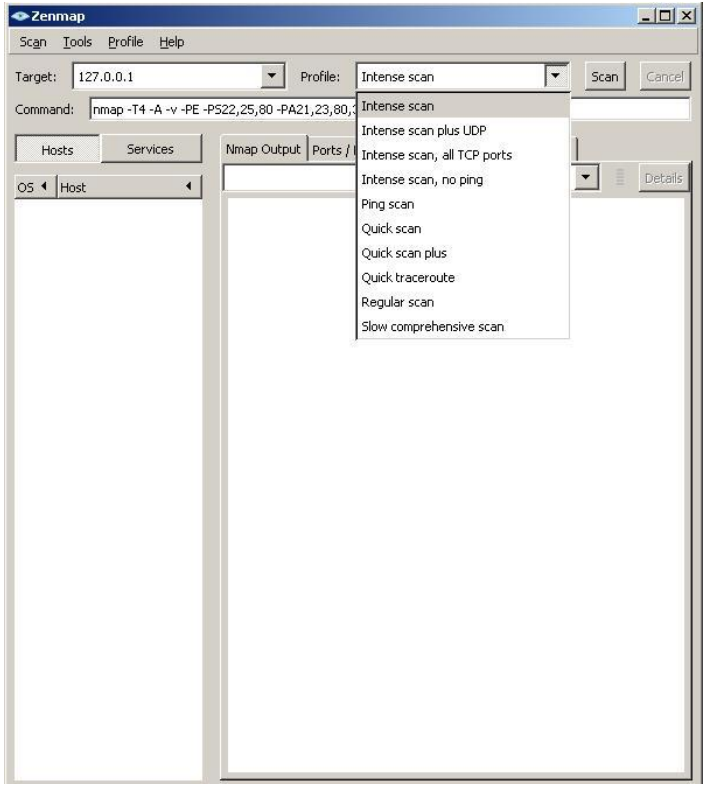
Covering Tracks

Nmap

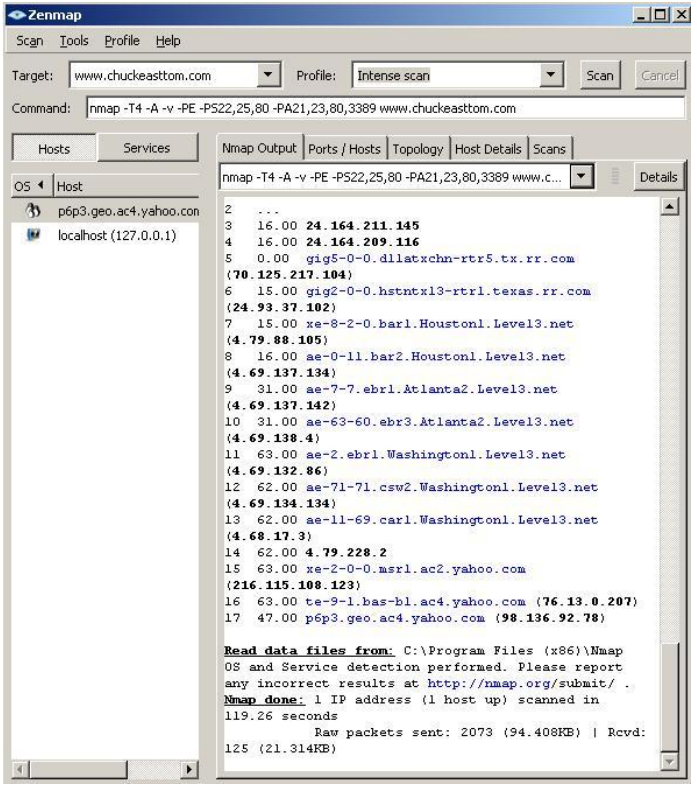
Nmap (network mapper)The most widely used port scanner

Can be extended with Nmap Scripting Engine (NSE) and Lua programming language

Nmap (ZenMap the GUI version)



Nmap Continued



NMAP Flags

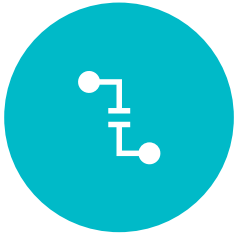
- -O detects operating system
- -sP is a ping scan
- -sT TCP connect scan
- -sS SYN scan
- -sF FIN scan
- -sX XMAS Tree scan
- -sN NULL Scan
- -sU UDP scan
- -sO Protocol Scan
- -sA ACK Scan
- -sW Windows Scan
- -sR RPC scan
- -sL List/DNS scan
- -sI Idle scan

- -Po Don't Ping
- -PT TCP ping
- -PS SYN ping
- -PI ICMP Ping
- -PB TCP and ICMP ping
- -PM ICMP netmask
- -oN Normal Output
- -oX XML output
- -oG Greppable output
- -oA all output
- -T timing
  - -T0 paranoid
  - -T 1 Sneaking
  - -T 2 Polite
  - -T 3 Normal
  - -T 4 Aggressive
  - -T 5 Insane

NMAP -continued

- Examples
  - Basic syn scan : nmap –sS 192.168.0.1
  - Basic Null scan : nmap –sN 192.168.0.1
  - Basic protocol scan: nmap –sO 192.168.0.1
  - Nmap stack fingerprinting: Nmap –O –p80<hosts>
  - Scan lower 1024 UDP Nmap –sU –p 1-1024 <hosts>
  - Scan a range of IP nmap 192.168.1.*
  - Scan IP v 6 nmap -6 IPv6-Address-Here
  - Show only open ports nmap --open 192.168.1.1

Types of Scans



Ping scan: This scan simply sends a ping to the target port. Many network administrators block incoming ICMP packets for the purpose of stopping ping scans.

SYN scan: This scan is very stealthy. Most systems accept SYN (Synchronize) requests. This scan is similar to the SYN flood DoS attack described in Chapter 4, “Denial of Service Attacks.” In this scan you send a SYN packet but never respond when the system sends a SYN/ACK. However, unlike the DoS SYN flood, you only send one packet per port. This is also called the *half-open scan*.

Connect scan: This is the most reliable scan, but also the most likely to be detected. With this type of scan a complete connection is made with the target system.

FIN scan: This scan has the FIN flag, or connection finished flag set. This is also not an unusual packet for systems to receive, so it is considered stealthy.

FLAGS

- In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:
- FIN = 1
- SYN = 2
- RST = 4
- PSH = 8
- ACK = 16
- URG = 32
- ECE = 64
- CWR = 128

Packet Flags

- CWR (1 bit) – Congestion Window Reduced (CWR) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in congestion control mechanism.
- ECE (1 bit) – ECN-Echo indicates
  - If the SYN flag is set, that the TCP peer is ECN capable.
  - If the SYN flag is clear, that a packet with Congestion Experienced flag in IP header set is received during normal transmission.
- URG (1 bit) – indicates that the Urgent pointer field is significant
- ACK (1 bit) – indicates that the Acknowledgment field is significant. All packets after the initial SYN packet sent by the client should have this flag set.
- PSH (1 bit) – Push function
- RST (1 bit) – Reset the connection
- SYN (1 bit) – Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags change meaning based on this flag, and some are only valid for when it is set, and others when it is clear.
- FIN (1 bit) – No more data from sender

- Note: SYN, FIN, ACK, URG, and RST are the flags most commonly used in port scanning.

Scan Responses

- FIN
  - Port closed response is RST
  - Port open no response
  - Windows PCs do not comply with RFC 793; therefore, they do not provide accurate results with this type of scan
- XMAS
  - Port closed response is RST
  - Port open no response
- SYN (considered stealthy, also called half open scan)
  - Port closed RST
  - IF the port is open, the target responds with a SYN-ACK. If it is closed, it responds with an RST
- NULL scan
  - All flags off
  - RFC 793 states that if a TCP segment arrives with no flags set, the receiving host should drop the segment and send an RST
- ACK Scan
  - If a port is filtered on a firewall, nothing comes back. If a port is unfiltered an RST is sent back.

Cisco has a great paper on port scanning
http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3

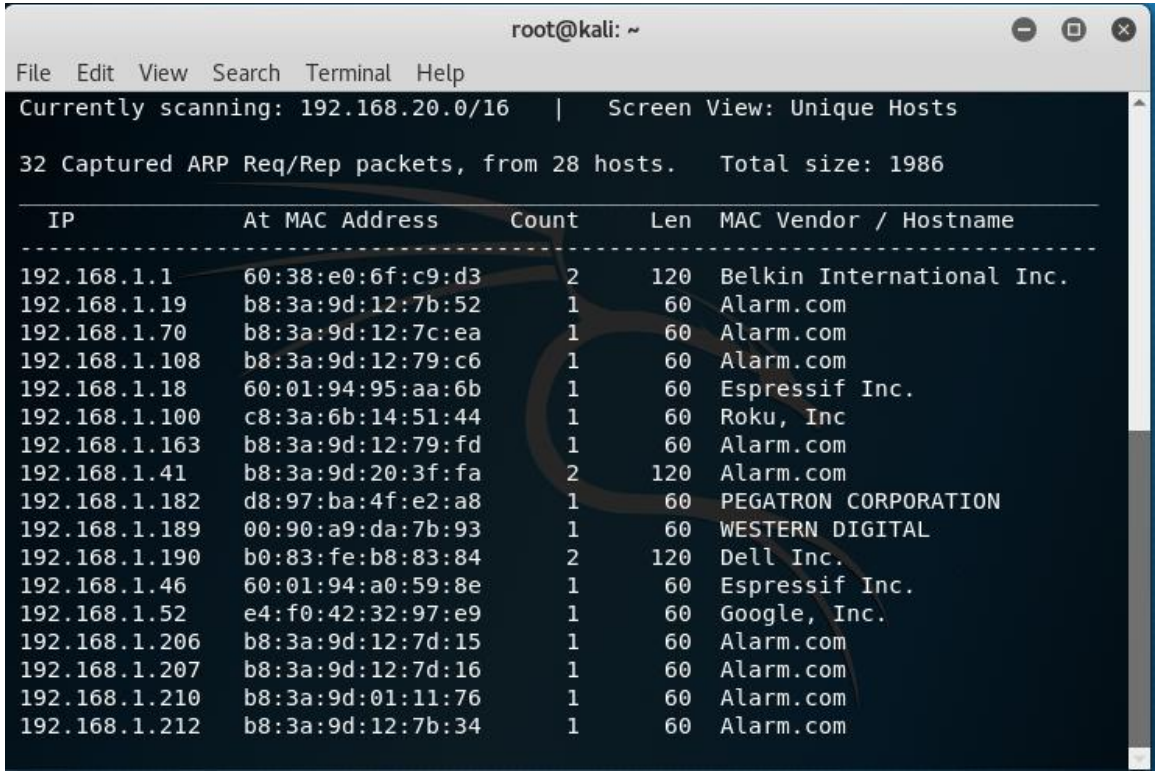
hping

- http://www.hping.org/
- Send TCP SYN packets to port 0 on host xyz.com
- hping xyz.com -S -V
- Send TCP SYN packets every 100,000 microseconds to port 443
- hping xyz.com -S -p 443 -i u100000

- -F –fin set FIN flag
  -S –syn set SYN flag
  -R –rst set RST flag
  -P –push set PUSH flag
  -A –ack set ACK flag
  -U –urg set URG flag
  -X –xmas set X unused flag (0x40)
  -Y –ymas set Y unused flag (0x80)

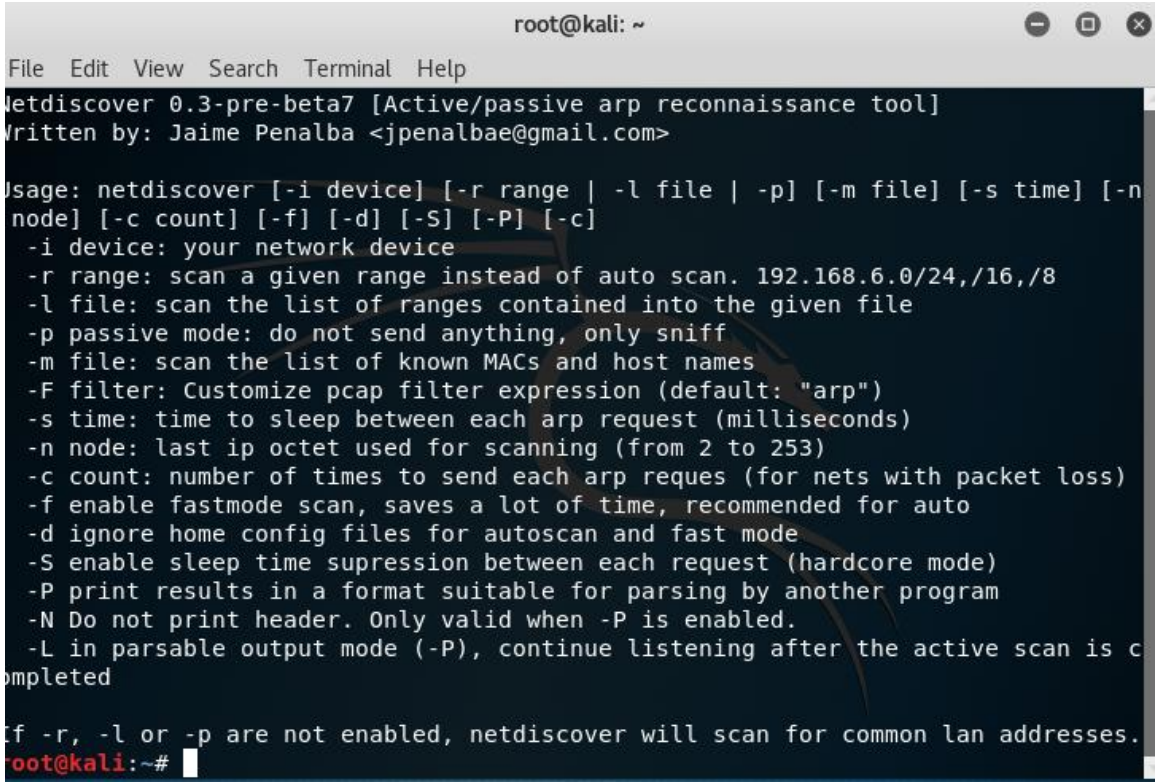
Netdiscover

Just netdiscover without any flags



Netdiscover

Flags



Netdiscover flags

-i device: your network device

-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8

-l file: scan the list of ranges contained into the given file

-p passive mode: do not send anything, only sniff

-m file: scan the list of known MACs and host names

-F filter: Customize pcap filter expression (default: "arp")

-s time: time to sleep between each arp request (miliseconds)

-n node: last ip octet used for scanning (from 2 to 253)

-c count: number of times to send each arp reques (for nets with packet loss)

-f enable fastmode scan, saves a lot of time, recommended for auto

-d ignore home config files for autoscan and fast mode

-S enable sleep time supression betwen each request (hardcore mode)

-P print results in a format suitable for parsing by another program

-N Do not print header. Only valid when -P is enabled.

-L in parsable output mode (-P), continue listening after the active scan is completed

Netdiscover examples

netdiscover -i eth0 -r 192.168.1.1/24

Netdiscover –r 192.168.1.1/24

Pre-test activites

RISK ASSESSMENT

SETTING CLEAR GOALS

DEFINING SCOPE

KNOW WHAT IS AND IS NOT BEING COVERED

PLAN TOOLS AND TECHNIQUES

Tools

- NetScan Tools Pro. Used for discovering network devices including IPv4/IPv6 address, host name, email address, etc.
- Other scanners
  - SuperScan
  - Network Inventory Explorer
  - Advanced Port Scanner
  - CurrPorts
  - MegaPing
  - Net Tools
  - IP-Tools
- Mobile Scanners
  - Ip Network Scanner
  - Fing
  - Umit Network Scanner
  - PortDroid
  - Pamn IP Scanner
  - Network Discovery

- Mobile Scanners
  - Ip Network Scanner
  - Fing
  - Umit Network Scanner
  - PortDroid
  - Pamn IP Scanner
  - Network Discovery

Port Scanning Counter Measures

Configure	Configure firewall and IDS to block probles
Block	Block ICMP
Perform	Perform your own scanning
Filter	Filter at routers
Update	Update router, IDS, and FIrewall

Netcat

A popular tool that is widely used by network administrators, hackers, and others.

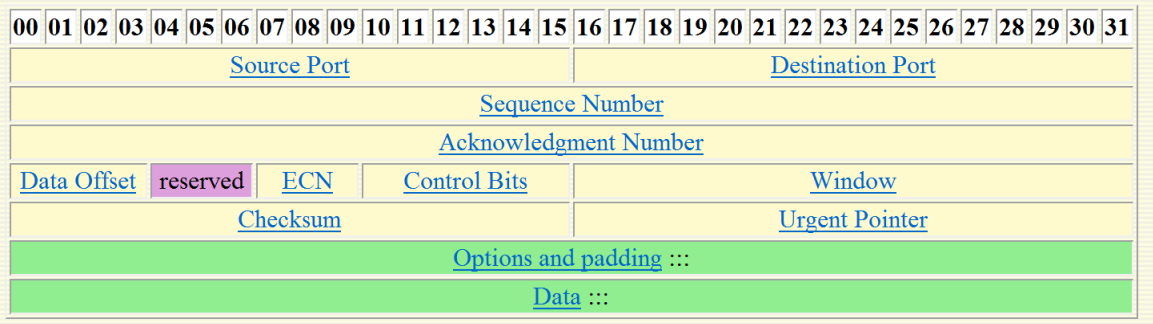
You can get it
http://netcat.sourceforge.net/

You can get netcat for Windows here
http://joncraton.org/blog/netcat-for-windows

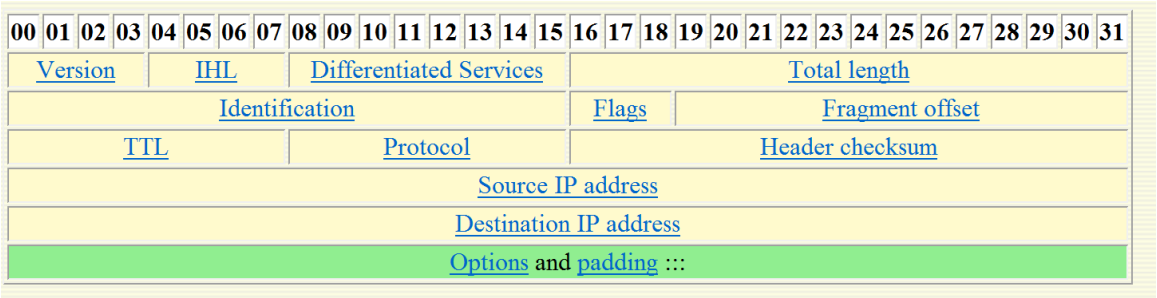
Netcat examples

- Listen on a given port
  - nc -l 3333
- Connect to listening port
  - nc 132.22.15.43 3333
- Connect to a mail server
  - nc mail.server.net 25
- Turn Netcat into a proxy server
  - nc -l 3333| nc www.google.com 80

Packet Structure - TCP Headers



Packet Structure - IP Headers



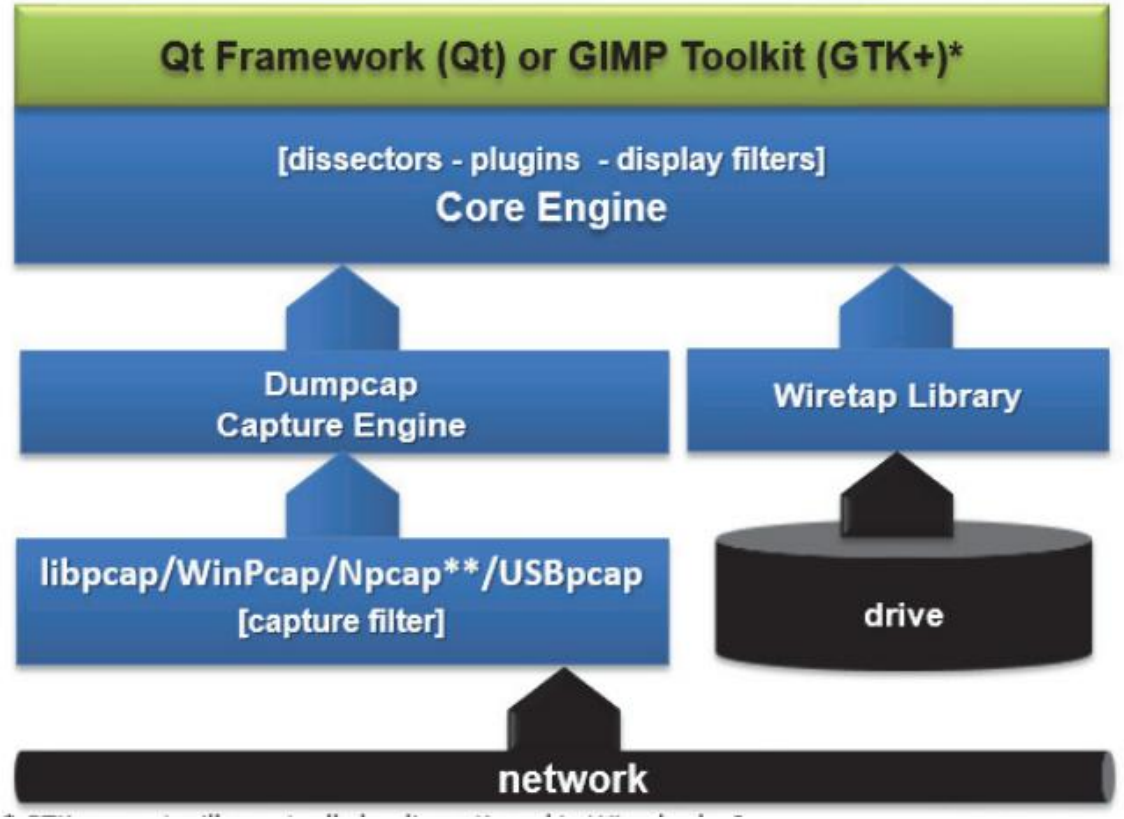
Packet Structure - Ethernet Header

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype or length	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets
	64–1522 octets							
72–1530 octets								
84–1542 octets								

Wireshark

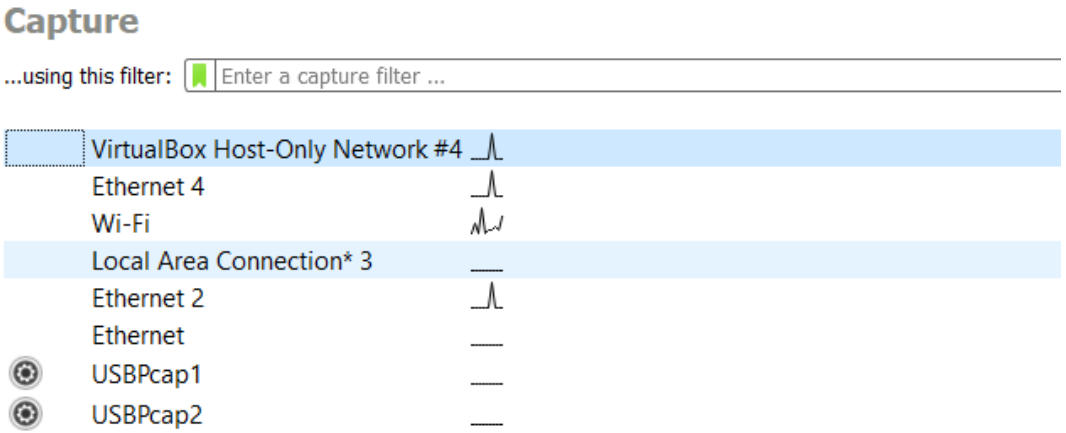
- Wireshark is one of the most widely known network packet sniffers. Often a penetration tester can learn a great deal from simply sniffing the network traffic on a target network. Wireshark provides a convenient graphical user interface (GUI) for examining network traffic. It is a free download, which you can get at https://www.wireshark.org/. tool can be downloaded for Windows or Macintosh

Wireshark

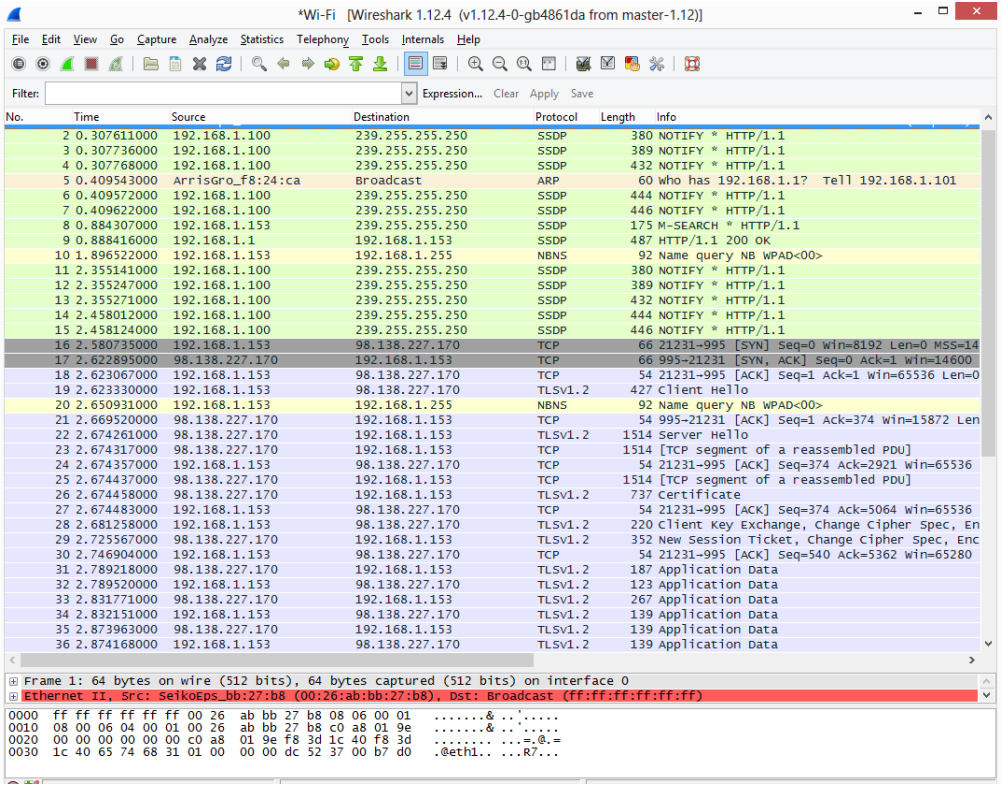

Qt Framework (Qt) or GIMP Toolkit (GTK+)*
[dissectors - plugins - display filters]
Core Engine
Dumpcap
Capture Engine
Wiretap Library
libpcap/WinPcap/Npcap**/USBpcap
[capture filter]
drive
network

Selecting something to capture

If you don't see traffic, it is not live.

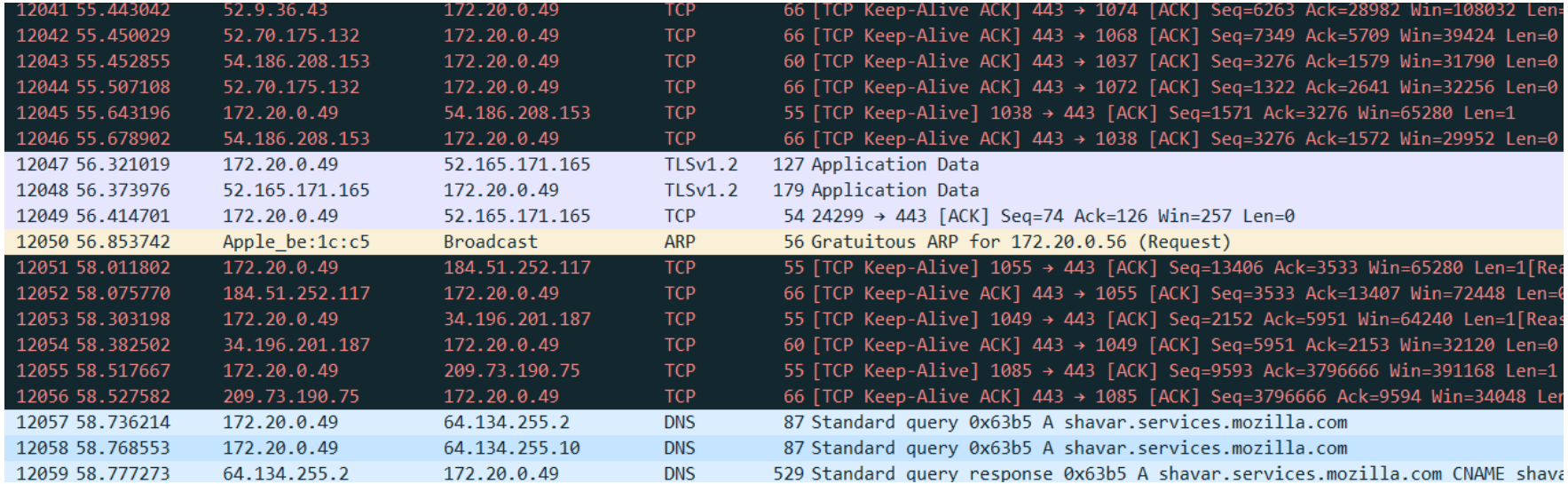


Analyzing network traffic



What do the colors mean

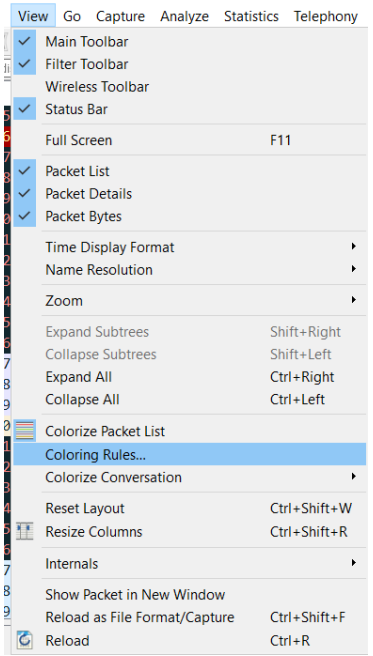
- Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems



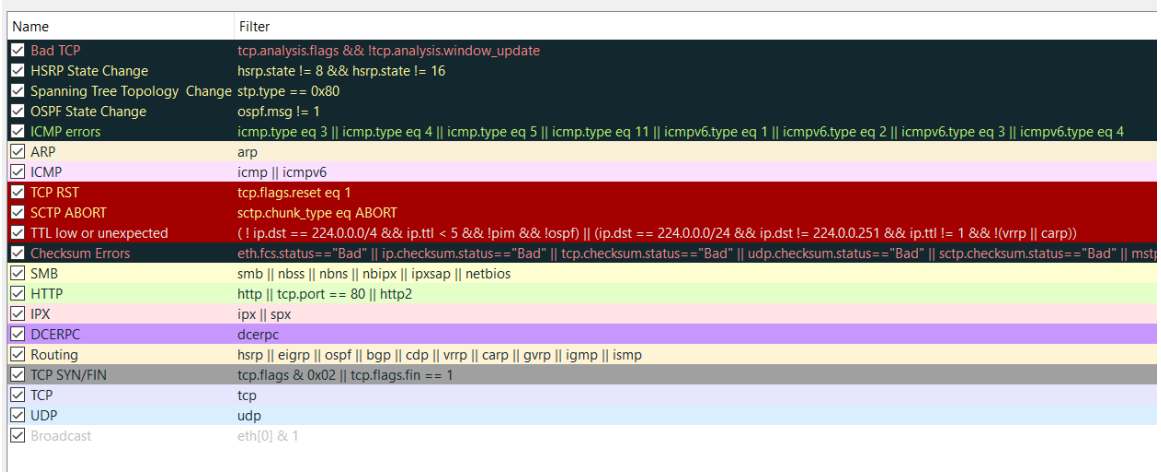
12041	55.443042	52.9.36.43	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1074 [ACK] Seq=6263 Ack=28982 Win=108032 Len=
12042	55.450029	52.70.175.132	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1068 [ACK] Seq=7349 Ack=5709 Win=39424 Len=0
12043	55.452855	54.186.208.153	172.20.0.49	TCP	60 [TCP Keep-Alive ACK] 443 → 1037 [ACK] Seq=3276 Ack=1579 Win=31790 Len=0
12044	55.507108	52.70.175.132	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1072 [ACK] Seq=1322 Ack=2641 Win=32256 Len=0
12045	55.643196	172.20.0.49	54.186.208.153	TCP	55 [TCP Keep-Alive] 1038 → 443 [ACK] Seq=1571 Ack=3276 Win=65280 Len=1
12046	55.678902	54.186.208.153	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1038 [ACK] Seq=3276 Ack=1572 Win=29952 Len=0
12047	56.321019	172.20.0.49	52.165.171.165	TLSv1.2	127 Application Data
12048	56.373976	52.165.171.165	172.20.0.49	TLSv1.2	179 Application Data
12049	56.414701	172.20.0.49	52.165.171.165	TCP	54 24299 → 443 [ACK] Seq=74 Ack=126 Win=257 Len=0
12050	56.853742	Apple_be:1c:c5	Broadcast	ARP	56 Gratuitous ARP for 172.20.0.56 (Request)
12051	58.011802	172.20.0.49	184.51.252.117	TCP	55 [TCP Keep-Alive] 1055 → 443 [ACK] Seq=13406 Ack=3533 Win=65280 Len=1[Rea
12052	58.075770	184.51.252.117	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1055 [ACK] Seq=3533 Ack=13407 Win=72448 Len=0
12053	58.303198	172.20.0.49	34.196.201.187	TCP	55 [TCP Keep-Alive] 1049 → 443 [ACK] Seq=2152 Ack=5951 Win=64240 Len=1[Reas
12054	58.382502	34.196.201.187	172.20.0.49	TCP	60 [TCP Keep-Alive ACK] 443 → 1049 [ACK] Seq=5951 Ack=2153 Win=32120 Len=0
12055	58.517667	172.20.0.49	209.73.190.75	TCP	55 [TCP Keep-Alive] 1085 → 443 [ACK] Seq=9593 Ack=3796666 Win=391168 Len=1
12056	58.527582	209.73.190.75	172.20.0.49	TCP	66 [TCP Keep-Alive ACK] 443 → 1085 [ACK] Seq=3796666 Ack=9594 Win=34048 Len
12057	58.736214	172.20.0.49	64.134.255.2	DNS	87 Standard query 0x63b5 A shavar.services.mozilla.com
12058	58.768553	172.20.0.49	64.134.255.10	DNS	87 Standard query 0x63b5 A shavar.services.mozilla.com
12059	58.777273	64.134.255.2	172.20.0.49	DNS	529 Standard query response 0x63b5 A shavar.services.mozilla.com CNAME shava

What do the colors mean

Go to View > Coloring Rules

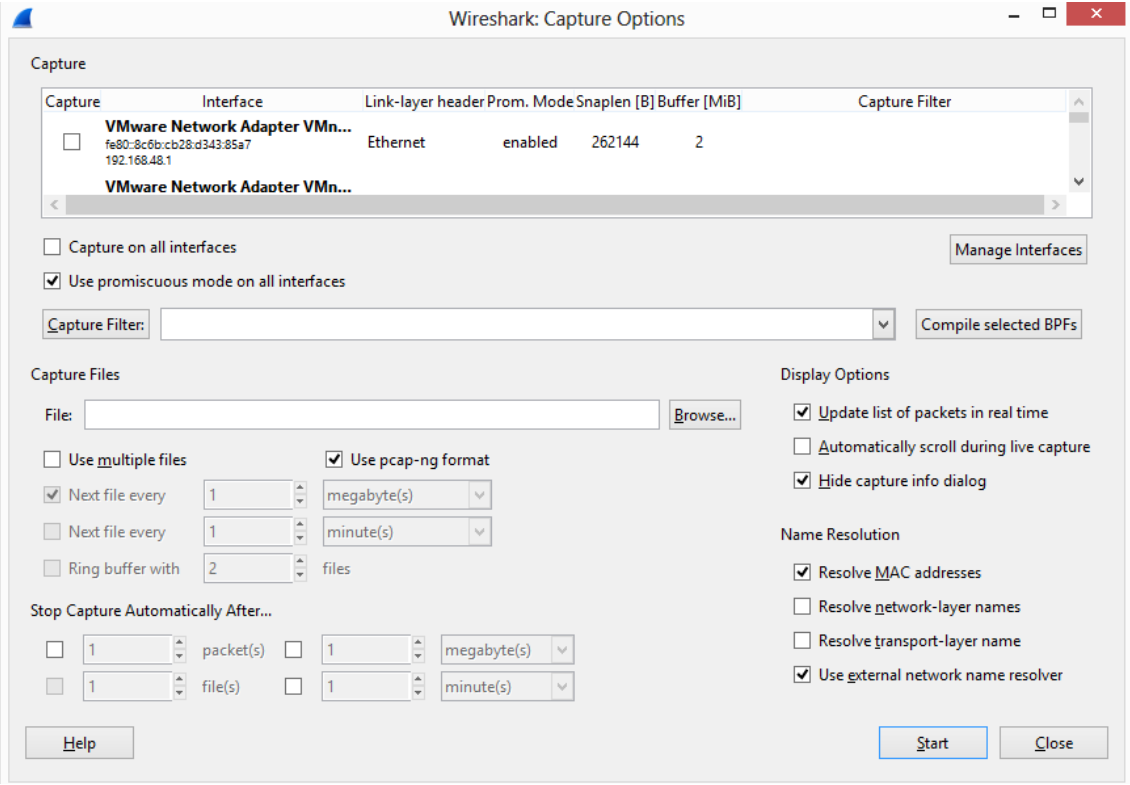


What do the colors mean

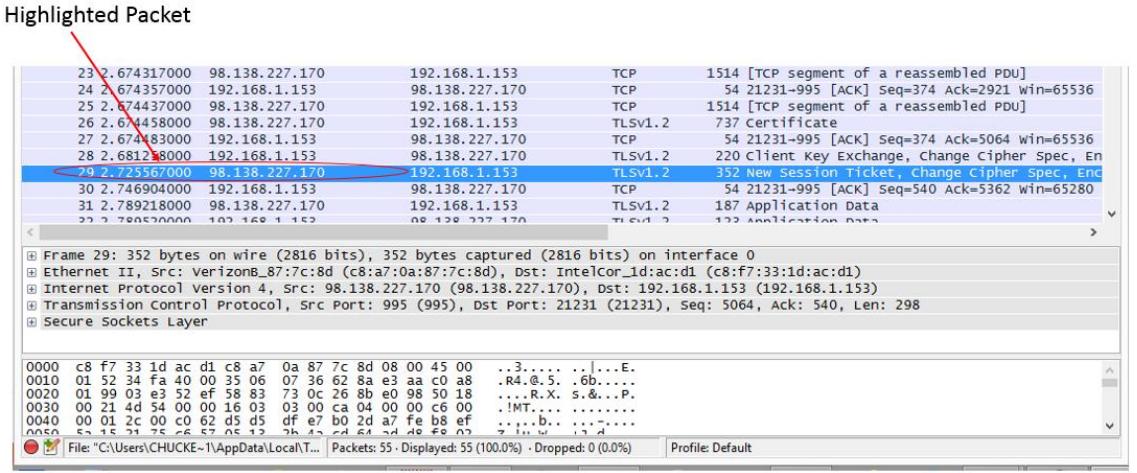


Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
ARP	arp
ICMP	icmp || icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp
SMB	smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP	http || tcp.port == 80 || http2
IPX	ipx || spx
DCERPC	dcerpc
Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1

Wireshark Configuration

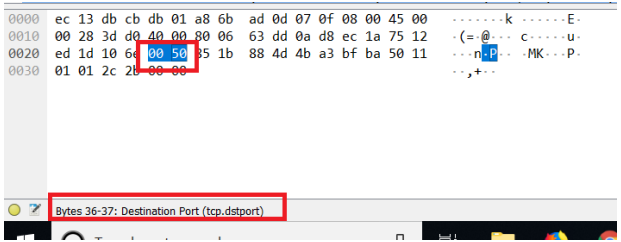


Wireshark Interface

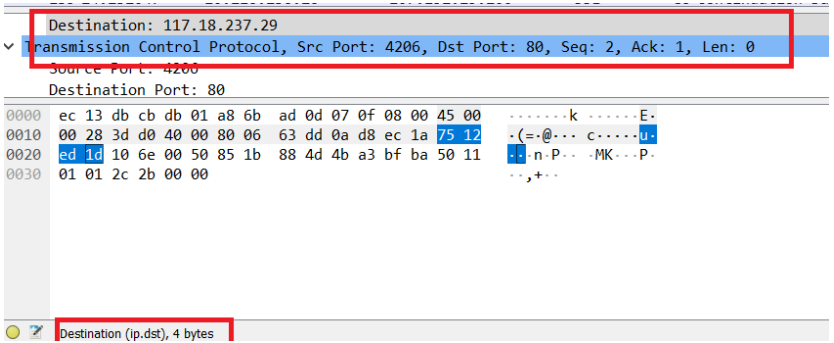


What are you looking at

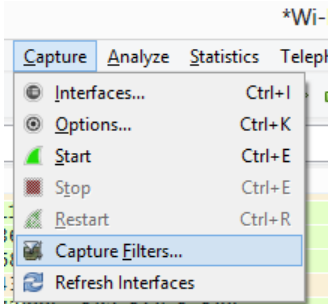
As you highlight items in the data pane, the content is described below

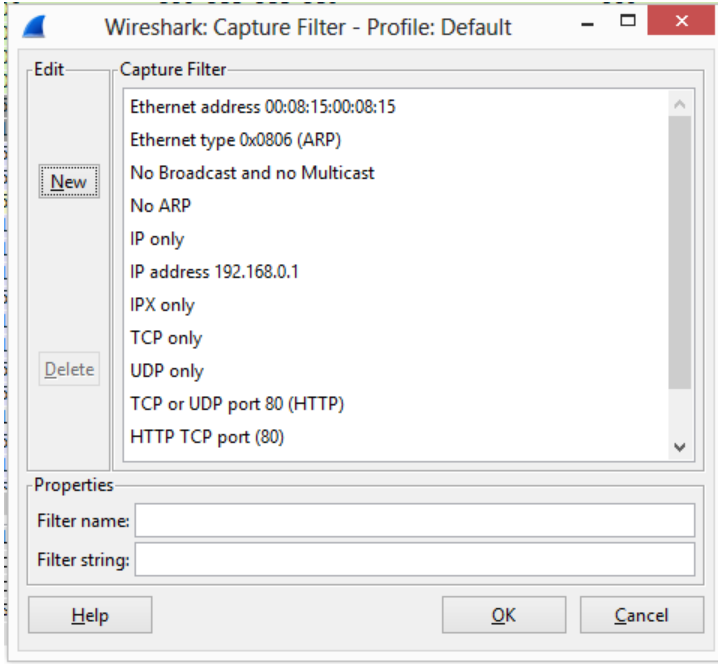


And if you click on it, then Details are shown above.



Capture Filter





Capture Filter examples

host 10.1.20.55

host 192.168.0.1 and host 10.1.20.55

tcp port http

ip

not broadcast not multicast

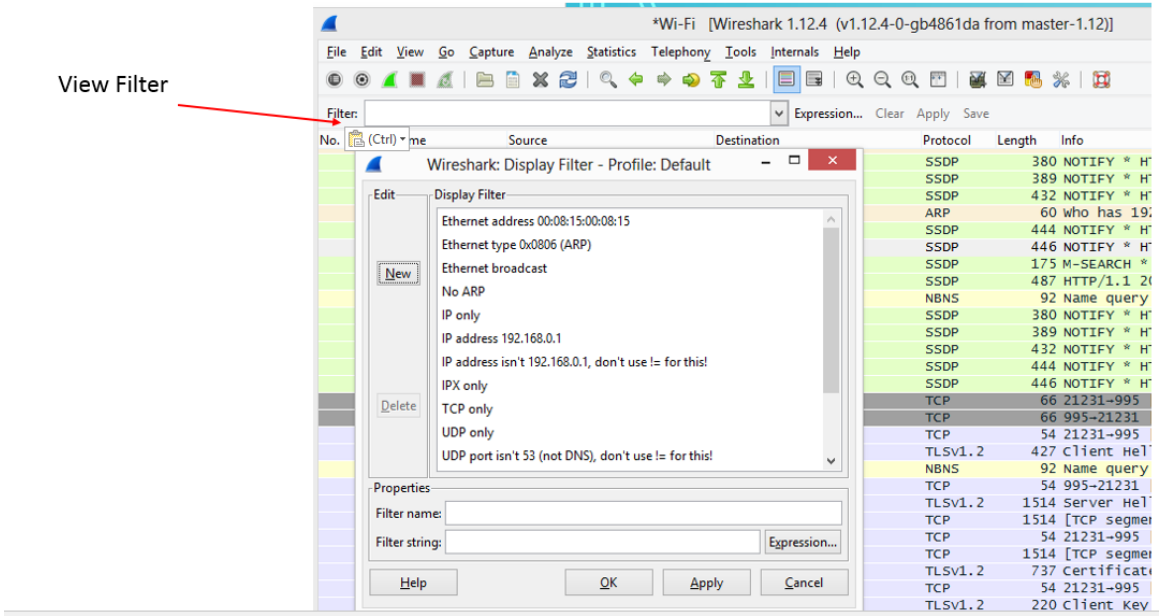
ether host 00:04:13:00:09:a3

Display Filters (Post-Filters)

Display filters (also called post-filters) only filter the view of what you are seeing. All packets in the capture still exist in the trace

Display filters use their own format and are much more powerful then capture filters

Display Filter



Display Filter Examples

ip.src==10.2.21.00/24

ip.addr==192.168.1.20 && ip.addr==192.168.1.30

tcp.port==80 || tcp.port==443

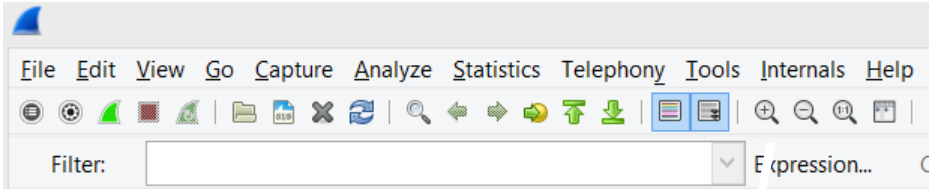
!(ip.addr==192.168.1.20 && ip.addr==192.168.1.30)

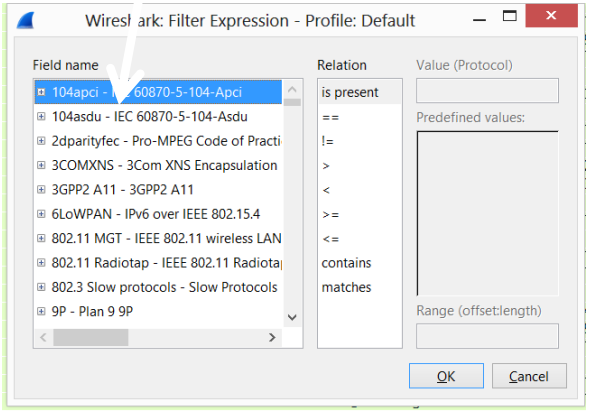
(ip.addr==192.168.1.20 && ip.addr==192.168.1.30) && (tcp.port==465|| tcp.port==139)

(ip.addr==192.168.1.20 && ip.addr==192.168.1.30) && (udp.port==80|| udp.port==443)

Display Filter

	Protocol	.	String 1	.	String 2	Comparison operator	Value	Logical Operations	Other expression
Syntax:									
Example:	ftp		passive		ip	==	10.2.3.4	xor	icmp.type



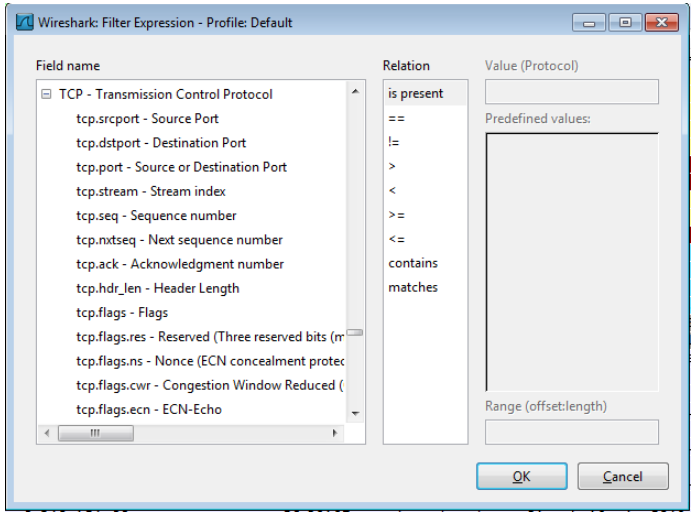


Display Filter

- String1, String2 (Optional settings):
  - Sub protocol categories inside the protocol.
  - Look for a protocol and then click on the "+" character.
  - Example:
  - **tcp.srcport == 80**
  - **tcp.flags == 2**
    - **SYN packet**
    - **Tcp.flags.syn==1**
  - **tcp.flags == 18**
    - **SYN/ACK**
  - **Note of TCP**

U	A	P	R	S	F
R	C	S	S	Y	I
G	K	H	T	N	N

:



Display Filter Expressions

- dns || icmp
  - Display the DNS or ICMP traffic.
- tcp.port == 443
  - Display packets with TCP source or destination port 443.
- tcp.flags
  - Display packets having a TCP flags
- tcp.flags.syn == 0x02
  - Display packets with a TCP SYN flag.

Six comparison operators are available:

English format:	C like format:	Meaning:
eq	==	Equal
ne	!=	Not equal
gt	>	Greater than
lt	<	Less than
ge	>=	Greater or equal
le	<=	Less or equal

➔ **Logical expressions**:

English format:	C like format:	Meaning:
and	&&	Logical AND
or	||	Logical OR
xor	^^	Logical XOR
not	!	Logical NOT

Correct syntax

Wrong syntax

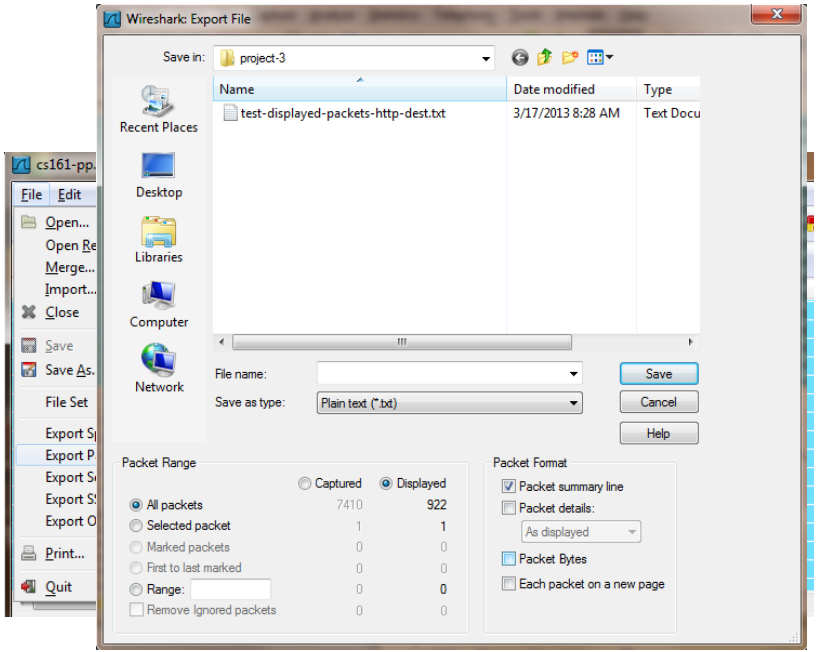
Save Filtered Packets After Using Display Filter

- We can also save all filtered packets in text file for further analysis
- Operation:

File→Export packet dissections →as “plain text” file

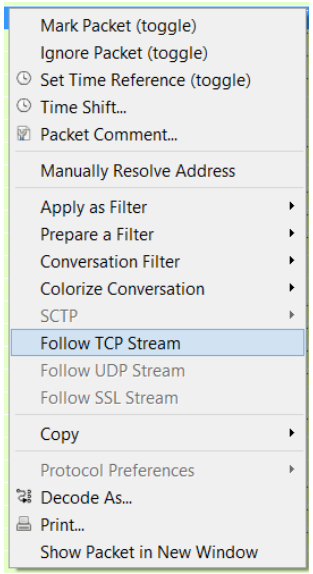
1). In “packet range” option, select “Displayed”

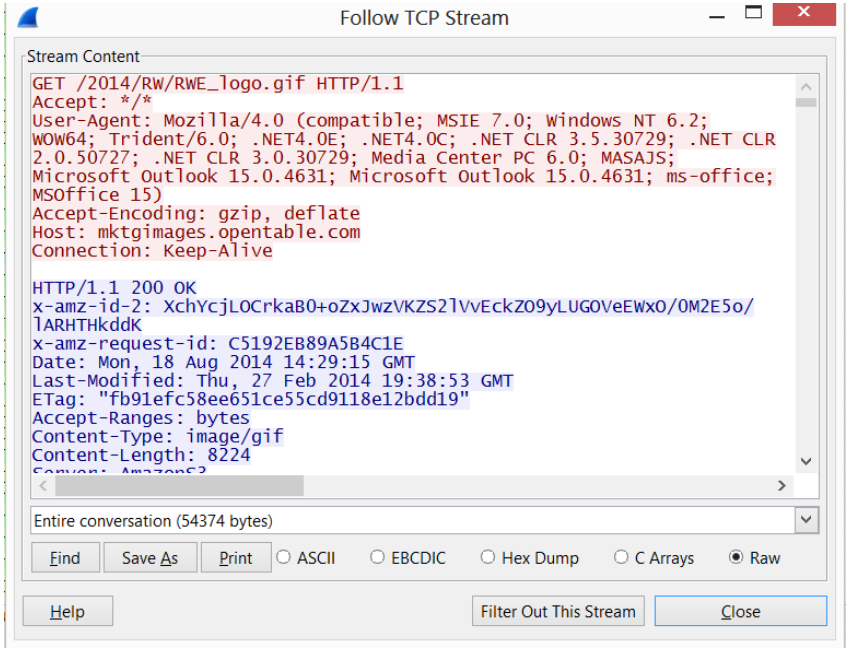
2). In choose “summary line” or “detail”



Follow TCP Stream

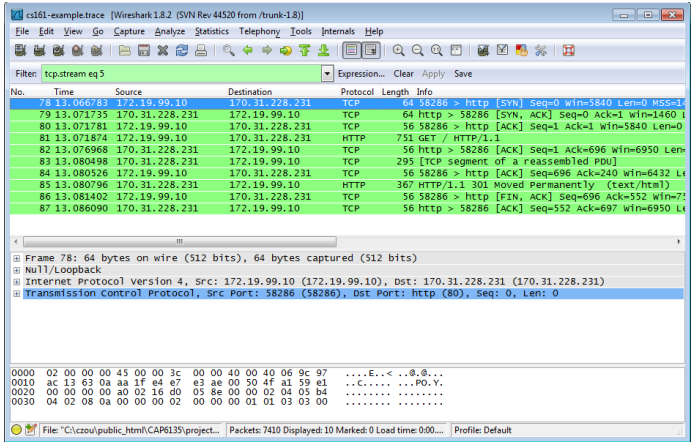
red - stuff you sent **blue - stuff you get**



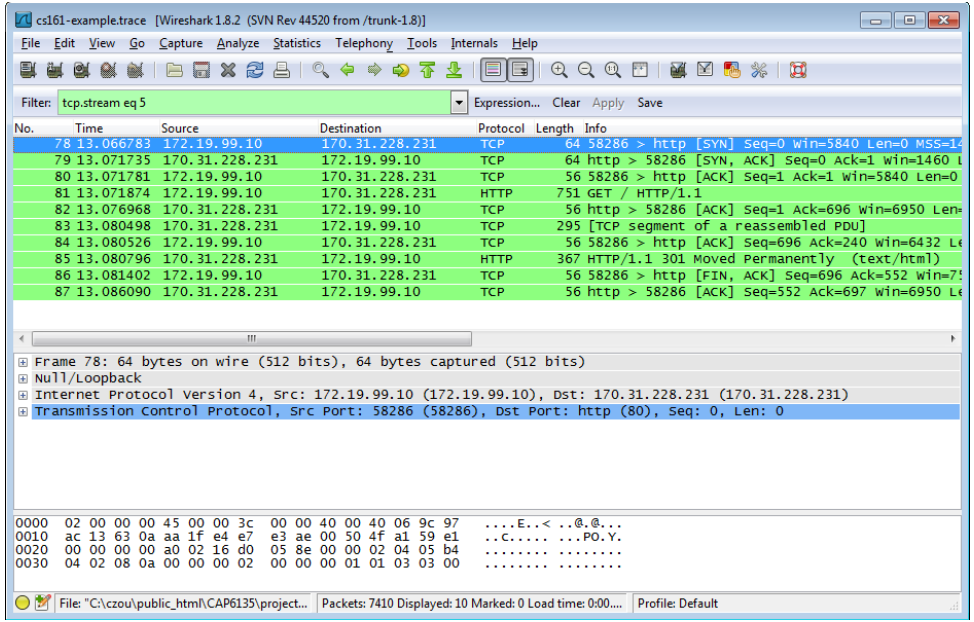


Filter out/in Single TCP Stream

- When click “filter out this TCP stream” in previous page’s box, new filter string will contain like:
  - http and !(tcp.stream eq 5)
- So, if you use “tcp.stream eq 5” as filter string, you keep this HTTP session

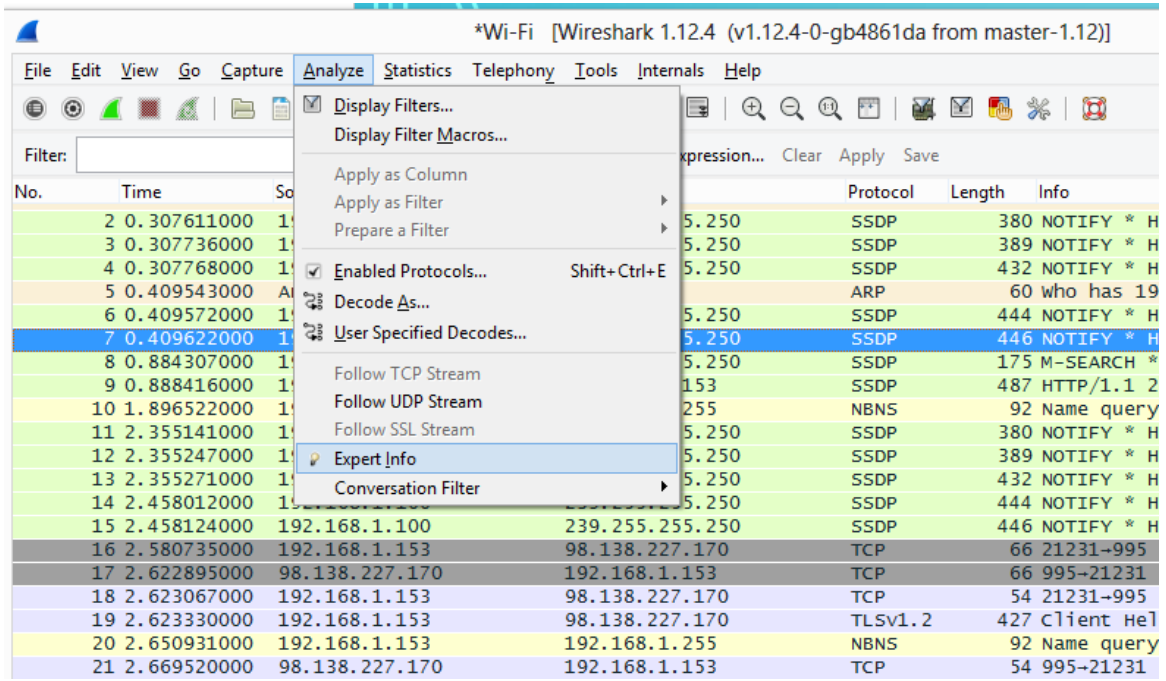


Filter out/in Single TCP Stream

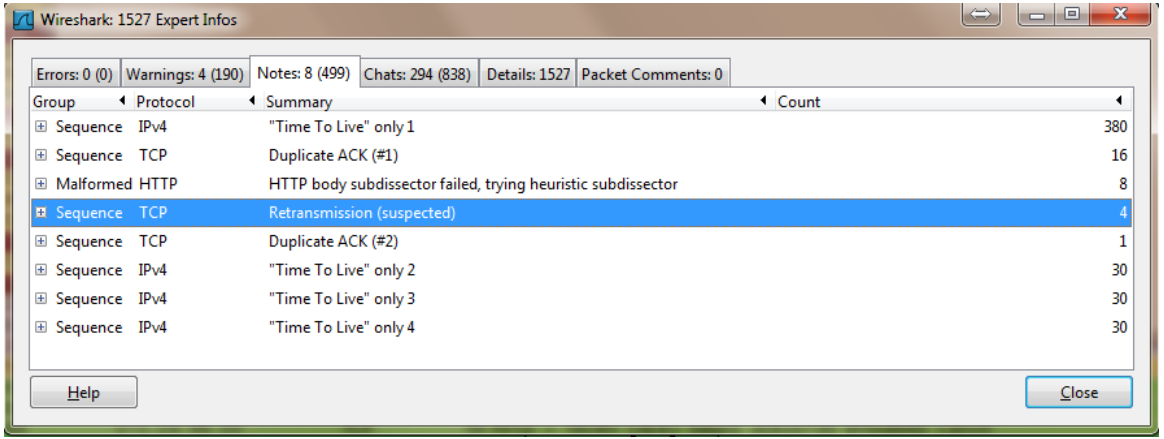


- When click “filter out this TCP stream” in previous page’s box, new filter string will contain like:
  - http and !(tcp.stream eq 5)
- So, if you use “tcp.stream eq 5” as filter string, you keep this HTTP session

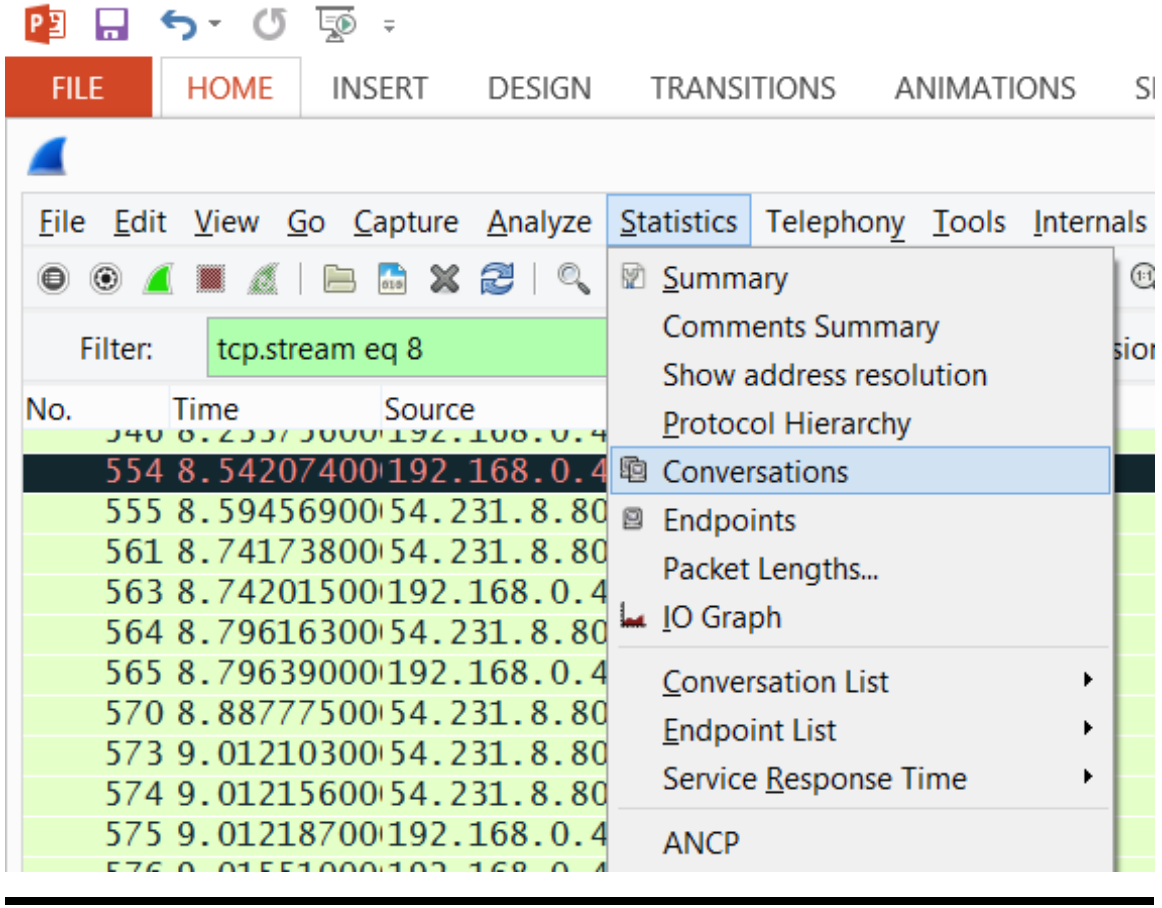
Expert Info


*Wi-Fi [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Conversation Filter
No. Time Protocol Length Info
2 0.307611000 SSDP 380 NOTIFY * H
3 0.307736000 SSDP 389 NOTIFY * H
4 0.307768000 SSDP 432 NOTIFY * H
5 0.409543000 ARP 60 Who has 19
6 0.409572000 SSDP 444 NOTIFY * H
7 0.409622000 SSDP 446 NOTIFY * H
8 0.884307000 SSDP 175 M-SEARCH *
9 0.888416000 SSDP 487 HTTP/1.1 2
10 1.896522000 NBNS 92 Name query
11 2.355141000 SSDP 380 NOTIFY * H
12 2.355247000 SSDP 389 NOTIFY * H
13 2.355271000 SSDP 432 NOTIFY * H
14 2.458012000 SSDP 444 NOTIFY * H
15 2.458124000 192.168.1.100 239.255.255.250 SSDP 446 NOTIFY * H
16 2.580735000 192.168.1.153 98.138.227.170 TCP 66 21231→995
17 2.622895000 98.138.227.170 192.168.1.153 TCP 66 995→21231
18 2.623067000 192.168.1.153 98.138.227.170 TCP 54 21231→995
19 2.623330000 192.168.1.153 98.138.227.170 TLSv1.2 427 Client Hel
20 2.650931000 192.168.1.153 192.168.1.255 NBNS 92 Name query
21 2.669520000 98.138.227.170 192.168.1.153 TCP 54 995→21231

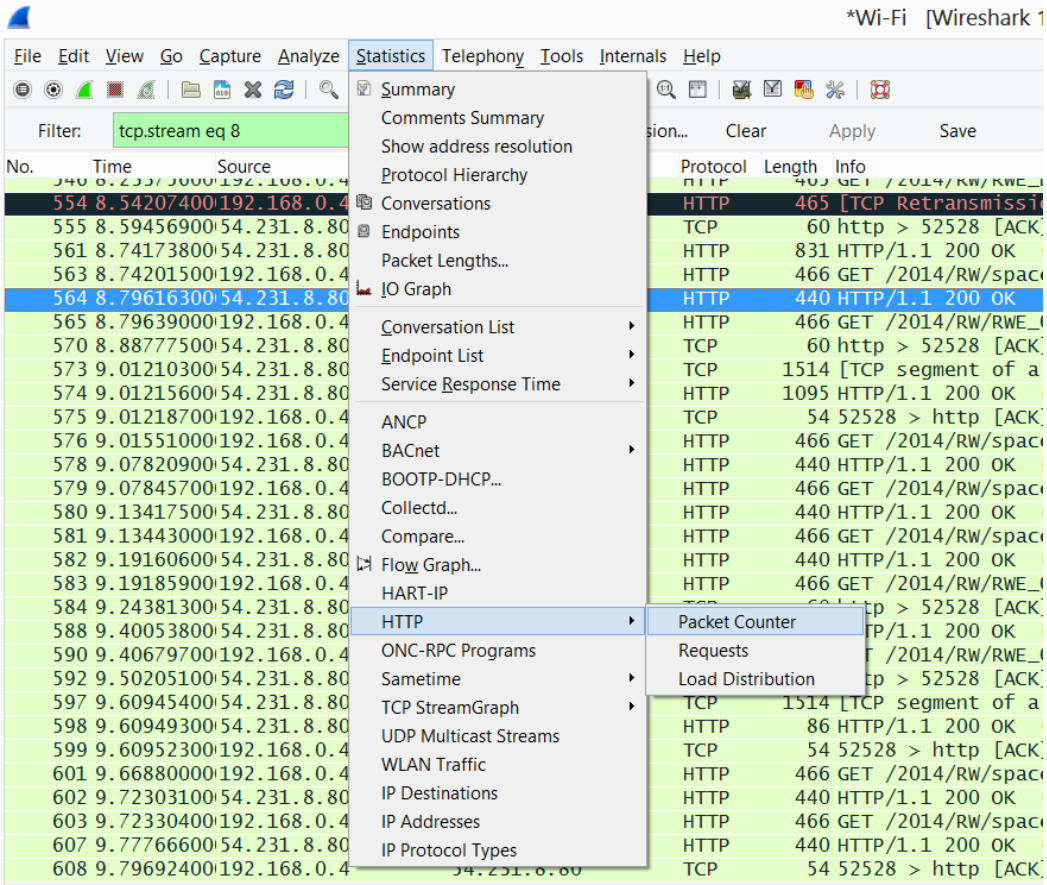
Expert Info


Wireshark: 1527 Expert Infos
Errors: 0 (0)
Warnings: 4 (190)
Notes: 8 (499)
Chats: 294 (838)
Details: 1527
Packet Comments: 0
Group
Protocol
Summary
Count
Sequence IPv4 "Time To Live" only 1 380
Sequence TCP Duplicate ACK (#1) 16
Malformed HTTP HTTP body subdissector failed, trying heuristic subdissector 8
Sequence TCP Retransmission (suspected) 4
Sequence TCP Duplicate ACK (#2) 1
Sequence IPv4 "Time To Live" only 2 30
Sequence IPv4 "Time To Live" only 3 30
Sequence IPv4 "Time To Live" only 4 30
Help
Close

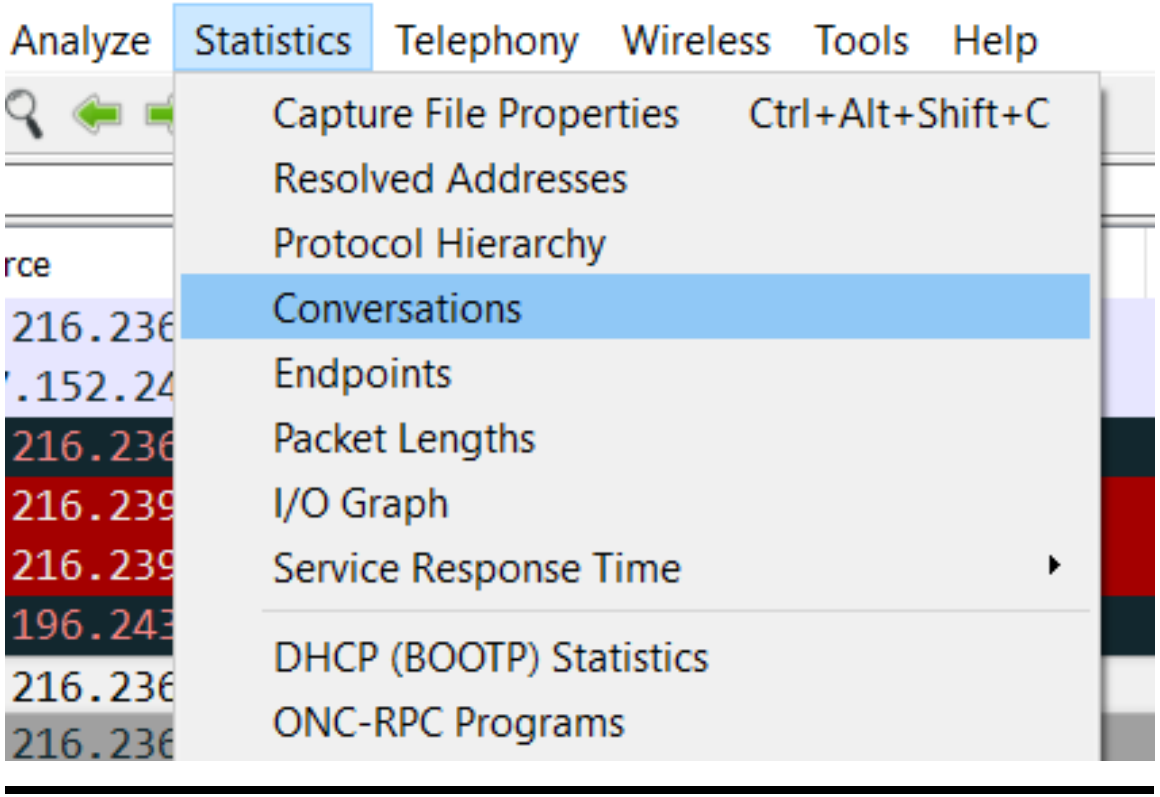
Conversations



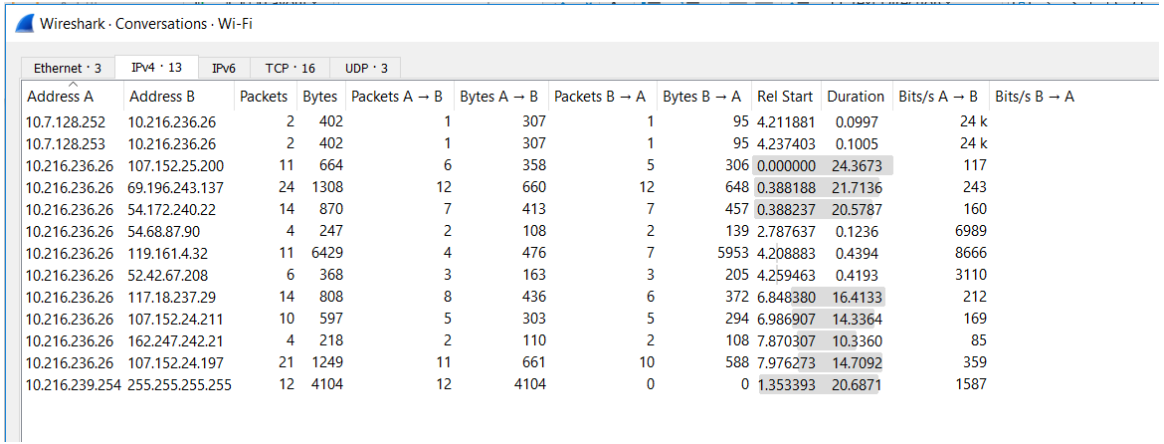
HTTP Analysis



View conversations



View conversations



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.7.128.252	10.216.236.26	2	402	1	307	1	95	4.211881	0.0997	24 k	
10.7.128.253	10.216.236.26	2	402	1	307	1	95	4.237403	0.1005	24 k	
10.216.236.26	107.152.25.200	11	664	6	358	5	306	0.000000	24.3673	117	
10.216.236.26	69.196.243.137	24	1308	12	660	12	648	0.388188	21.7136	243	
10.216.236.26	54.172.240.22	14	870	7	413	7	457	0.388237	20.5787	160	
10.216.236.26	54.68.87.90	4	247	2	108	2	139	2.787637	0.1236	6989	
10.216.236.26	119.161.4.32	11	6429	4	476	7	5953	4.208883	0.4394	8666	
10.216.236.26	52.42.67.208	6	368	3	163	3	205	4.259463	0.4193	3110	
10.216.236.26	117.18.237.29	14	808	8	436	6	372	6.848380	16.4133	212	
10.216.236.26	107.152.24.211	10	597	5	303	5	294	6.986907	14.3364	169	
10.216.236.26	162.247.242.21	4	218	2	110	2	108	7.870307	10.3360	85	
10.216.236.26	107.152.24.197	21	1249	11	661	10	588	7.976273	14.7092	359	
10.216.239.254	255.255.255.255	12	4104	12	4104	0	0	1.353393	20.6871	1587	

Ngrep

- Ngrep
  - Download from http://ngrep.sourceforge.net/download.html
  - Examples
    - Monitor any traffic using port 443
      - ngrep -d any port 443
    - Capture traffic on eth0 with HTTP GET or POST
      - ngrep -l -q -d eth0 -i "^GET |^POST " tcp and port 80

  Ngrep man page http://linux.die.net/man/8/ngrep

ISACA CISA Definition for Audit

- “Systematic process by which a qualified, competent, independent team or person objectively obtains and evaluates evidence regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented.”

Auditor Qualifications

- **Independent:**
- **Professional Independence**: Auditor acts independent of group being audited
- No friendships, dating, suggestive language, parties, lunches
- **Organizational Independence**: Auditor and his/her organization has no special interest in the audited organization
- **Qualified, Competent:**
- Adhere to Professional Ethics Standard
- ISACA standard and professional care
- Professional Competence
- Has skills/knowledge to complete task
- Continued professional training/education

Terms used in Audits

Control: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

IT Control Objective: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Evidence: Evidence is any information used by the auditors whether the entity or data being audited follows the established audit criteria or objective.

IT Governance: A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes

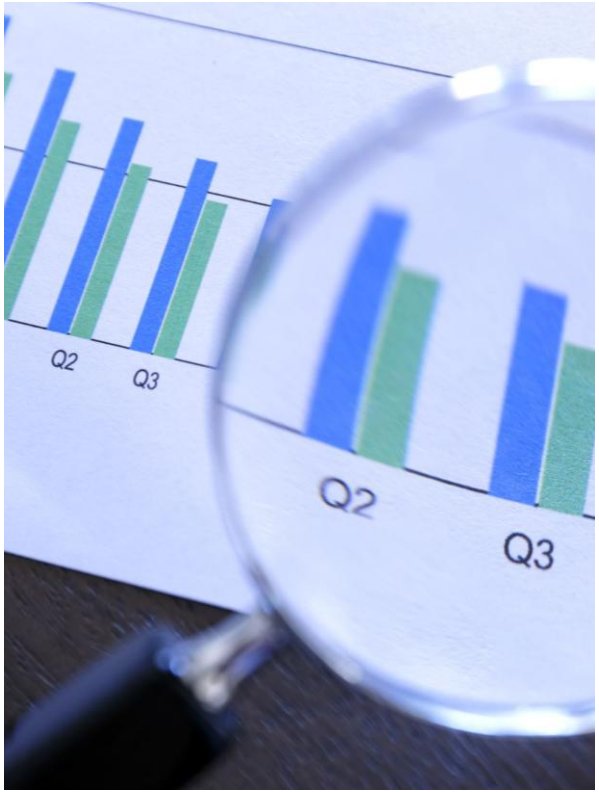
Control Self-Assessment (CSA

- Control Assessment can be defined as a “management technique that assures stakeholders, customers and other parties that internal control system of the organization is reliable. It also ensures that employees are aware of the risks to the business and they conduct periodic, proactive reviews of control.

Substantive v Compliance Testing

- **Compliance Testing**:
- Are controls in place and consistently applied?
- Access control
- Program change control
- Procedure documentation
- Program documentation
- Software license audits
- System log reviews
- Exception follow-ups

- **Substantive Testing**:
- Are transactions processed accurately?
- Are data correct and accurate?
- Double check processing
- Calculation validation
- Error checking
- Operational documentation
- If Compliance results are poor, Substantive testing should increase in type and sample number



Compliance Testing

- Control: Is production software controlled?
- Test: Are production executable files built from production source files?
- Test: Were proper procedures followed in their release?
- Control: Is Sales DB access constrained to Least Privilege?
- Test: Are permissions allocated according to documentation?
- Test: When sample persons access DB, can they access only what is allowed?

Substantive Testing

Audit: Is financial statement section related to sales accurate?

Test: Track processing of a sample transactions through the system, performing calculations manually

Test: Test error conditions

Audit: Is tape inventory correct?

Test: Search for sample days and verify complete documentation and tape completeness

Sampling

Statistical Sampling:

- N% of all items randomly tested
- Should represent population distribution

Variable Sampling: How accurate is the sample population in matching the full population?

- Determine appropriateness of sampling: (e.g., $, weight, amount): Sample average $24.50, Real average: $26.99

No statistical (or Judgment) Sampling:

- Auditor justifies another distribution for sample selection
- Which items are most risky?

Sampling

- **Tolerable Error Rate**: The maximum allowable error rate (e.g., inappropriately documented changes)
- **Non-Statistical Sampling** includes**:**
- **Discovery Sampling**: A minimal testing model used when the expected occurrence rate is extremely low (e.g., find fraud, break laws)
- **Stop-or-Go Sampling**: If the first 20 have zero errors, then stop. Else if the first 100 have < 10 errors, stop. Else…
- **Attribute Sampling**: How many of X have Y attribute?
- E.g. How many changes are appropriately documented?