

Mag. iur. Dr. techn. Michael Sonntag

Collecting information

E-Mail: sonntag@fim.uni-linz.ac.at http://www.fim.uni-linz.ac.at/staff/sonntag.htm Institute for Information Processing and Microprocessor Technology (FIM) Johannes Kepler University Linz, Austria

© Michael Sonntag 2013



- E I M
 - NMap
 - Web caches
 - Web Archive
 - Whols
 - MX-Records
 - Wireshark

NMap

- NMap (Network MAPper) is a network scanner
 - → It tries to find all computers in a specific network and checks what ports are open, what OS they are running, whether there is a firewall, etc.
- It does not look for specific vulnerabilities!
 - → But it gives recommendations; e.g. services to disable
 - \rightarrow Some scans + vuln. systems \rightarrow Lock-up/crash!
- Used as a tool for inventory generation in a network
 - → Are there any computers which should not be there?
 - → Can also be used to gather information for a later attack » Which OS/software and which version is running
- Stages: 1 = Host discovery, 2 = Port scan, 3 = Service/ version detection, 4 = OS detection, 5 = Scripting

 \rightarrow Scripting may also include vulnerability/malware detection!

NMap and forensics

- To gather an "inventory" of what exists
 - \rightarrow Computers \rightarrow Try to find them physically, if they show up!
 - \rightarrow Services \rightarrow If port 22 is open, but no SSH server is running,
 - you should investigate the computer in detail
 - » Hint at a rootkit, which hides itself
 - » Similar for "normal" and "public" services:
 - Should they be running?
 - What are they doing?
 - Advantage: Happens from outside & from a trusted computer
 - If the port is open, this cannot be hidden as e.g. from netstat!
- Where to find information on ports?
 - → C:\Windows\System32\drivers\etc\services » Name, TCP, and/or UDP; sometimes a comment
 - → Google for the "unofficial" uses
 - → Official: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml
 - See also: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

• Usage:

- → Start program and enter IP address
- → Select profile for scanning
 - » Special options only available in the command line version or when constructing a new profile!
- Your tasks:
 - → Install NMap (+ the UI Zenmap)
 - → Scan the local subnet for hosts »Use a "Quick scan"
 - → Scan the machine of your neighbour » Use a "Regular scan"
 - \rightarrow Interpret the results
 - » Correct output?
 - » Something surprising/dangerous found?

Sample result: NMap local subnet scan

		-M	Sample result
f	-	$\Pi \leq $	NMap local subnet sca
1	Fl		
ľ		👁 Zenmap	
		Sc <u>a</u> n Werkzeuge <u>P</u> rofil	Hife
		Ziel: 140.78.100.128/25	▼ Profil: Ping scan ▼ Scan Abbrechen
		Befehl: nmap -sn 140.78.10	0.128/25
		Rechner Dienste	Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans
		Betriebssystem • Rechner	nmap -sn 140.78.100.128/25 Details
		I r1-intern.f	MAC Address: 00:11:85:C9:62:A0 (Hewlett Packard)
		hp2824-1a	Mildin Nmap scan report for npic3f08e.fim.uni-linz.ac.at (140.78.100.138) host is up (0.0020s latency).
		mpic3f08e	<pre>fm.u Nmap scan report for hpljm602.fim.uni-linz.ac.at (140.78.100.140)</pre>
		hpljm602.1	Host is up (0.00s latency).
		praher-vis	MAC Address: 20:76:8A:3E:A0:E2 (Unknown)
		inge_xp.a	Host is up (0.00s latency).
		₩ 140.78.10	
		sabine-win	Host is up (0.0010s latency).
		140.78.10	Nmap scan report for 140.78.100.168
		140.78.10	Host is up (0.0030s (atency).
		michael_w	Nmap scan report for sabine-win7.ads2-fim.fim.uni-linz.ac.at (140.78.100.205)
		jrm_win7.a	Mac Address 50:50:50:51:57:02 (Unknown)
			Nmap scan report for 140.78.100.206
			MAC Address: 00:22:15:A9:DD:A1 (Asustek Computer)
		140.78.10	Nmap Scan report for 140.78.100.200
			Host is up (0.00s latency). MAC Address: 40:6C:8F:46:EB:48 (Unknown)
			Nmap scan report for michael_w7.ads2-fim.fim.uni-linz.ac.at (140.78.100.211)
			Host is up. Nmap scan report for jrm_win7.ads2-fim.fim.uni-linz.ac.at (140.78.100.212)
			Host is up (0.00s latency).
			MAC Address: E0:69:95:12:CD:15 (Unknown) Nmap scan report for 140.78.100.250
			Host is up (0.0030s latency).
			MAC Address: 00:04:23:D3:FB:5C (Intel) Nmap scan report for 140.78.100.251
			Host is up (0.00s latency).
		4	MAC Address: 00:04:23:D3:FB:5A (Intel) Nmap done: 128 IP addresses (14 hosts up) scanned in 2.73 seconds
		Filtere Rechner	militar utile. 120 ir autresses (14 hosts up) scaliled in 2.73 seconds

F		M	
	Rechnerl	betrachter	
		Allgemein Dienste Traceroute	
	router	Allgemeine Informationen	
	inge_s habib.t	Adresse: [pv4] 140.78.100.31	-
	jrm_w:	Rechnername: [PTR] router.fim.uni-linz.ac.at	-
	hplj41(hp282- hp282-	Betriebssystem	
	hp262)	Benutzte Ports: 1/tcp dosed	<u> </u>
	alex_v praher	Klasse Fingerabdruck	
	cs140-	% (Vendor (Type (Family (Version)	
	140.7t	100 Cisco router IOS 12.X	
	fim_ma	100 Cisco switch IOS 12.X	
	hoer_>		
	npi805	Reihen	

Rechner	Rechnerbetrachter								
Hosts	Allgemein Dier	nste Tracero	ute						
r1-inte	Dente (E)	(00F	بالمستعاد	u					
router.	Ports (5) Ex	traports (995) Speziairei	der					
inge_s	Port 4	Protocol 4	State 🔍	Service 4	Method				
habib.t	1 35	tcp	filtered	msrpc	table				
jrm_w:	135	state	reason_ip						
hplj41(135	state	state	filtered					
hp282	135	state	reason						
hp282	135	state	reason_ttl						
hp262	135	service	product						
alex_v	135	service	name	msrpc					
praher	135	service	extrainfo	<spezialfeld></spezialfeld>					
cs140-	135	service	version						
140.78	135	service	conf	3					
fim_ma	135	service	method	table					
hoer_	± 139	tcp	filtered	netbios-ssn	table				
npi805	± 445	tcp	filtered	microsoft-ds	table				
In Internet	F 502	ten	filtered	http://www.enman	tahla				

pD4	M	Sample resu
F		NMap in
	🗢 Zenmap	
	Scan Werkzeuge Profil Hilfe	
	Ziel: 140.78.100.31 Profil: Comprehensive	Scan Abbrechen
	Befehl: nmap -sS -sU -sV -T4 -O -A -v -PE -PM -PP -PS -PA -PU -PO -PY 140.78.100.31	
	Rechner Dienste Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details	Scans
	Betriebssystem Rechner router.fi Kommentare	
	hp2824 Geöffnete Ports: 0	
	hp2824- Gefilterte Ports: 5	
	Market Ma	
	pi8054 Gescannte Ports: 1000 Laufzeit: Not available	
	jrm_w7. Letzter Systemstart: Not available	u
	Mabib.fin	
	Malex_v6- IPv4: 140.78.100.31	
	hoer_xp IPv6: Not available	
	MAC: Not available	
1	CS140-7	
	fim_mad Name - Typ: router.fim.uni-linz.ac.at - PTR praher-v	
	son_vist	
	140.78.	
	🕨 inge_sta	
	Filtere Rechner	

	ſ	- M	/	Sample	e resi
ĺ	PL	<u>IJ</u> S		N	Map ii
ļ		Zenmap			
			euge <u>P</u> rofil <u>i</u>		Although an
		· · · · · · · · · · · · · · · · · · ·	3.100.31		Abbrechen
		Befehl: nma	p -sS -sU -sV -T4	4-O-A-v-PE-PM-PP-PS-PA-PU-PO-PY 140.78.100.31	
		Rechner	Dienste	Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans	
		Betriebssyster	n • Rechner	nmap -sS -sU -sV -T4 -O -A -v -PE -PM -PP -PS -PA -PU -PO -PY 140.78.100.31	Details
			router.fi	Discovered open port 161/udp on 140.78.100.31	
			r 1-intern	Completed UDP Scan at 15:21, 814.93s elapsed (1000 total ports) Initiating Service scan at 15:21	
			hp2626-	Scanning 5 services on router.fim.uni-linz.ac.at (140.78.100.31)	
			hp2824-	Service scan Timing: About 60.00% done; ETC: 15:23 (0:00:51 remaining) Completed Service scan at 15:22, 77.51s elapsed (5 services on 1 host)	
			hp2824-	Initiating OS detection (try #1) against router.fim.uni-linz.ac.at (140.78.100.31)	
			hplj4100	Initiating Traceroute at 15:22 Completed Traceroute at 15:22, 0.01s elapsed	
				Initiating Parallel DNS resolution of 2 hosts. at 15:22	
		-	npi8054	Completed Parallel DNS resolution of 2 hosts. at 15:22, 0.00s elapsed	
			jrm_w7.	NSE: Script scanning 140.78.100.31. Initiating NSE at 15:22	
			habib.fin	Completed NSE at 15:23, 5.01s elapsed	
	1		alex_v6	Nmap scan report for router.fim.uni-linz.ac.at (140.78.100.31)	
			hoer_xp	Host is up (0.00024s latency). Not shown: 1984 closed ports	
			alex_w2	PORT STATE SERVICE VERSION	
			cs140-78	135/tcp filtered msrpc 139/tcp filtered netbios-ssn	
	0		fim_mad	445/tcp filtered microsoft-ds	
			praher-v	593/tcp filtered http-rpc-epmap	
			son_vist	1434/tcp filtered ms-sql-m 67/udp open/filtered dhcps	
			140.78.	123/udp open ntp NTP v4	
			inge sta	ntp-info: receive time stamp: 05/17/11 15:23:01	
			inge_ata	system: cisco	
				I leap: 0	

	M	Sample re	su
Ē		NMap	in
	Filtere Rechner	<pre>1134/top filtered ms=sql=m 67/dp open filtered dhcps 123/udp open ntp NTP v4 intp=info: i receive time stamp: 05/17/11 15:23:01 i system: cisco i leap: 0 i stratum: 4 i rootdelay: 4.33 i rootdispersion: 49.09 i peer: 34814 i refid: 140.78.2.62 i refime: 0xb17CF524.5EB5F39E i poll: 6 i clock: 0xb17CF524.5EB5F39E i poll: 6 i clock: 0xb17CF531.5D3A7B03 i phase: 0.212 i freq: 28.90 i prefiltered mstpc 135/udp filtered mstpc 135/udp filtered metbios=ns 161/udp open smmp Cisco SNMP service i_smmp=vin32=shares: TIMSOUT 162/udp open[filtered mstpc] 133/udp filtered mstpc] 134/udp filtered mstpc] 135/udp filtered mstpc] 134/udp filtered mstpc] 134/ud</pre>	

Google Cache

- The cache gives you access to old/removed content
 - \rightarrow Which might still be applicable!
- Attention: Surfing the cache will still touch the server
 - → E.g. images are loaded from the "source"
- Way around: View the text-only version
 - → Add "&strip=1" to the search URL
- Not necessarily complete: Some elements or pages might not be cached (recently/at all)
 - \rightarrow Also: Only the last version is available!
- Access:
 - → Google search
 - → Directly: "cache: <URL>"
 - » E.g. "cache:www.jku.at"

Google cache: Tasks

- Visit the Google cache for the FIM course homepage » Hint: Search words "fim linz lva teaching"
 - → Check where the FIM logo comes from and what this would mean regarding traces of your actions
 - » How can you prevent this? Test and document it!
 - → Identify the date of this version
 - → Compare this version with the original one » How would you do this?
 - » Note: We want a real comparison, not "looks the same"!
 » What problems do occur? How can you reduce them?
- Investigate, whether Bing and Yahoo do have a similar feature; if yes, try it and document the differences!
 - → Both in features and for the specific page above!

Web archive: Tasks

- Web Archive (=Wayback Machine) is a permanent archive of the WWW (not: The Internet!)
 - → Find out which pages are being archived, and how often!
 - → What is archived for a web page? Check the logo!
 - \rightarrow How reliable is it, i.e. which modifications take place?
- "I don't want my page in there!"
 - → What can you do?
 - → Is this permanent?
- Try the archive with the following URL: http://www.fim.uni-linz.ac.at/Lva/default.htm
 - → What is the oldest version?
 - » Is this really the oldest one?
 - Try to get the page without any additions (Wayback-header)! » Hint: Search the FAQ!

Web archive: Solution

- Not everything is archived: Often only the web page (=HTML) alone, but not any images, ...
 - \rightarrow Especially not if from a different domain!
- Exclusion: By robots.txt file
 - → According to posts this is not permanent: "blocked" pages are just not shown, but not deleted!
 - \rightarrow Later on removed \rightarrow Content is visible (again)!
 - → Might lead to "new" content being not retrieved/stored
- Pages are rewritten (e.g. links) \rightarrow This is not a forensic copy!
 - → "Original" version: Append "id_" to date/number
 - → Note: Images are then retrieved from the current server!

DNS/Whols

- Find a web-based tool for DNS information
 - → Investigate the owner of "www.jku.at"
 - » But think about this question before entering it!
 - → Can you also find the history of this domain? » How would this be possible?
 - \rightarrow Who owns this domain?
- Get information on the host "www.jku.at"
 - Both via web tools as well as your own computer! » And repeat this at home from within your private network!

DNS/Whols

- http://whois.domaintools.com
- www.jku.at is useless: Only "jku.at" is in the NIC.at!
 - → Regarding www: Ask the JKU!
- History: Not accessible
 - → Ask the NIC.at (doubtful whether it even exists)
 - Or use a commercial database (unclear whether included)
 - \rightarrow You would have to regularly store a copy
- Owner: "Johannes Kepler Universitaet"
- www.jku.at
 - → Might have a different IP from inside the university and outside
 - → Outside: Proxies might be involved (not necessarily visible!)

DNS/Whols – MX records

- E-Mail information
 - → Where would E-Mails to "michael.sonntag@jku.at" be sent? » And where so "sonntag@fim.uni-linz.ac.at"?
 - \rightarrow How would you find this out?
 - → Explain the difference between this and the information about "www.jku.at"!
 - → From where (which IP address) would you expect to receive E-Mails sent from this address?

» Is there any possibility to find out?

- MX Lookup from within the institute (see next slide):
 - → Why the difference?
 - » Explain it!
 - » Discuss why this is important for computer forensics!
 - \rightarrow What does this mean for E-Mail header interpretation?

DNS/Whols – MX records

-							
	C:\Windows\system32\cmd.exe - nslookup	_ 🗆 ×					
	Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	_					
	C:\Users\michael>nslookup Default Server: edc1.ads2-fim.fim.uni-linz.ac.at Address: 140.78.100.119						
	> set type=mx > jku.at Server: edc1.ads2-fim.fim.uni-linz.ac.at Address: 140.78.100.119						
	Non-authoritative answer: jku.at MX preference = 10, mail exchanger = mail2.edvz.uni-linz.ac.at jku.at MX preference = 10, mail exchanger = mail1.edvz.uni-linz.ac.at jku.at MX preference = 5, mail exchanger = mail3.edvz.uni-linz.ac.at						
	mail2.edvz.uni-linz.ac.at internet address = 140.78.3.69 mail1.edvz.uni-linz.ac.at internet address = 140.78.3.68 > fim.uni-linz.ac.at Server: edc1.ads2-fim.fim.uni-linz.ac.at Address: 140.78.100.119						
	fim.uni-linz.ac.at MX preference = 20, mail exchanger = mail2.edvz.uu .ac.at	ni-linz					
	fim.uni-linz.ac.at MX preference = 5, mail exchanger = smtp.fim.uni-: .at	linz.ac					
	fim.uni-linz.ac.at MX preference = 10, mail exchanger = mail1.edvz.u	ni-linz					
	.ac.ai mail2.edvz.uni-linz.ac.at internet address = 140.78.3.69 smtp.fim.uni-linz.ac.at internet address = 140.78.100.121 mail1.edvz.uni-linz.ac.at internet address = 140.78.3.68 >	-					

F

DNS/Whols – MX records

ac.at >> -t MX NOERROR,	NS/Whols - MX
>> -t MX NOERROR,	fim.uni-linz.ac.at , id: 9067
>> -t MX NOERROR,	, id: 9067
NOERROR	, id: 9067
MX	
MV	20 mail2.edvz.uni-linz.ac.at.
	10 mail1.edvz.uni-linz.ac.at.
NS	alijku01.edvz.uni-linz.ac.at.
	ns1.fim.uni-linz.ac.at.
NS	ns2.fim.uni-linz.ac.at.
	140.78.3.68
	140.78.3.69
AAAA	2001:628:2010:2::69
	140.78.100.48
	140.78.3.62
A	140.78.2.62
	MX MX MX NS NS NS NS NS A AAAA A AAAA A A AAAA A A A

DNS/WhoIs – MX records

- MX for "jku.at": mail{1,2,3}.edvz.uni-linz.ac.at
 - \rightarrow Primarily mail1 and equally to mail2 and mail3
- MX for "fim.uni-linz.ac.at": smtp.fim.uni-linz.ac.at or mail1/mail2.edvz.uni-linz.ac.at
 - \rightarrow Primarily to FIM, then mail1, then mail2
 - → Different view from the outside: Everything must go through the university mail server and is then sent on!
- Outgoing: Sent from the FIM mailserver to destination directly, i.e. NOT using the JKU mailserver!
- Different views are possible and do exist

DNS/WhoIs – MX records

- Why? JKU can delegate subdomains itself. This happened to fim.uni-linz.ac.at
 - → Note: Different domain, but principles for "jku.at" apply to "uni-linz.ac.at" as well!
- Received E-Mails: Same address
 - → Especially: FIM ("smtp"!)
 - → But: Not necessarily! Outbound mails might not be scanned and just be sent from any internal address (JKU has public IPs; else: NAT!)

» JKU is large: Might have a separate server for sending

Wireshark

- If you want to see the real traffic from/to a computer, you need to listen in on the wire!
- \rightarrow Listening on the computer itself is not a good idea » Requires time \rightarrow Modification of behaviour » Binaries (or even the network driver) might be modified \rightarrow Listening on the default gateway/router » Will only show traffic going there/outside » Internal traffic will mostly go directly (no bus topology + switch) → What can you do? » Special wiretap devices (=copy traffic to a second port) » Network monitoring port on switches (=copy traffic on spec. port) » Listen on the system itself or on the router 🙂 Software for this:
 - → Wireshark: UI + interpretation of protocols + …

→ tcpdump: Unix commandline tool with little additional functions Michael Sonntag

- Wireshark is a network sniffer
 - → Available for Windows and Linux
- It will make a "copy" of every incoming and outgoing packet and present it to you
 - → This would not be that useful...
- It also parses a lot of protocols
 - → So no binary display (also available!), but
 - \rightarrow layer 3 display (IP addresses, port numbers, ...),
 - → up to layer 5 (actual http content as text/binary file)
- Practical problem: Network traffic is very large & frequent
 - → Filtering is an absolute necessity or anything useful will get lost in a torrent of uninteresting traffic!

Common display filtering expressions (1)

- Operators: == != < > <= >= && || ^^ !
 - → [...] or [....] or [...-]: Offset / Offset:Length / Offset-End » Only possible as comparison, e.g. eth.src[0:3]==08:15:47!
- Layer 1/2: frame.??? / eth.???, arp.???, ppp.???
 - → Usually not very interesting
- Layer 3: ip.???, ipv6.???, icmp.???, icmpv6.???
 - Examples ip.???: .src, .dst, .addr, .src_host, .dst_host, .host, .flags, .fragment, .len, .proto, .ttl

» ip.tos, ip.tos.cost, ip.tos.delay, ip.tos.precedence, ip.tos.reliability, ip.tos.throughput

- → Examples icmp.???: .code, .type, .mtu
- Layer 4: tcp.???, udp.???
 - → Examples tcp.???: .syn, .ack, .fin, .checksum, .flags, .len, .srcport, .dstport, .port, .time_delta, .window_size
 - Examples udp.???: .srcport, .dstport, .port, .length

See also: http://packetlife.net/library/cheat-sheets/

Common display filtering expressions (2)

• Layer 5: http, ospf, rip, ...

→ Examples http.???

 accept, .accept_encoding, .accept_language, .cookie, .date, .host, .last_modified, .location, .referer, .request, .request.method, .request.uri, .response, .response.code, .server, .set_cookie, .user_agent, .transfer_encoding

- Attention: This means that packets have been received and are stored, but will not be shown in the graphical UI!
 - \rightarrow There is also the possibility of filtering-before-storing
 - These are "capture filters", which use the syntax on libpcap (or tcpdump, which is the same)

» Examples: ether host 08:15:47:11:CA:FE

- Display filter for the same: eth.addr=08.15.47.11.CA.FE
- » Note: Too many packets to store \rightarrow Some might be lost
- » But: Capture filter dropped it \rightarrow Gone forever

Wireshark: Capture Options	
Capture	
Interface: Local Intel(R) PRO/100 VE Net	etwork Connection: \Device\NPF_{400
IP address: fe80::a400:fe81:4022:2a12, 140.78.100.211	
Link-layer header type: Ethernet	Wireless Settings
Capture packets in promiscuous mode	Remote Settings
Capture packets in pcap-ng format (experimental)	Buffer size: 1 tmegabyte(s)
Limit each packet to 1 bytes	
Capture Filter:	•
Capture File(s)	Display Options
File: Browse	Update list of packets in real time
Use multiple files	
Mext file every 1 megabyte(s)	Automatic scrolling in live capture
Next file every 1 minute(s)	Hide capture info dialog
✓ Ring buffer with 2 states	
Stop capture after 1	Name Resolution
Stop Capture	Enable MAC name resolution
I after 1	Enable network name resolution
I after 1 megabyte(s)	·
in after in minute(s)	Enable transport name resolution
Help	<u>S</u> tart <u>C</u> ancel

- Interface: Select where to listen
- Capture filter: Throw away packets before handling/storing them
- Capture file: How/where to store data; especially useful for keeping a history (e.g. last 60 minutes), timing, ...
- Buffer size: 1 MB can be too small for fast interface, much traffic and large packets!
- Display options: Personal prefer.
- Name resolution: Be careful!
 - → This might cause additional traffic!

- Usage:
 - → Start program and select interface to monitor
 - → Investigate content while running (difficult) or stop the scan and the start evaluation (store to disk, ...)
- Your tasks:
 - → Install Wireshark
 - Might require reboot for the packet capturing library!
 - \rightarrow Start a scan of your local interface
 - » Note: Wireless can be difficult/require additional libraries!
 - → Ping your neighbour & analyze the traffic
 - → Navigate to a website & analyze the traffic
 - → Log in to this website through a form (unencrypted)
 » Analyze the traffic
 - → Do the same as before, but now using a TLS connection!

er: Time	× 2 ≟ ○ ↔ ↔ 3 7 		् 🖭 i	🏽 🗹 🍢 🔆 🛛	
Time		Expression Clear Apply			
	Source	Destination	Protocol	Info	
1 0.000000	Intel_76:be:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174	
2 0.174052 3 0.579412	e0:69:95:12:cd:15 HewlettP_c9:64:72	Broadcast Spanning-tree-(for-k	ARP	who has 140.78.100.138? Tell 140.78.100.212 RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
4 0.864438	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129	
5 0.999988	Intel_76:be:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174	
6 1.854523	Intel_40:e1:0d	Broadcast	ARP	Who has 140.78.100.138? Tell 140.78.100.129	
7 2.158932 8 2.160081	140.78.100.211 140.78.100.140	140.78.100.140 140.78.100.211	ICMP ICMP	Echo (ping) request Echo (ping) reply	
9 2.579815	HewlettP_c9:64:72	Spanning-tree-(for-k		RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
10 2.854583	Intel_40:e1:0d	Broadcast	ARP	Who has 140.78.100.138? Tell 140.78.100.129	
11 3.149568 12 3.150553	140.78.100.211 140.78.100.140	140.78.100.140 140.78.100.211	ICMP ICMP	Echo (ping) request Echo (ping) reply	
13 4.149606	140.78.100.140	140.78.100.140	ICMP	Echo (ping) request	
14 4.150692	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
15 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	- 7
16 4.580183 17 5.149709	HewlettP_c9:64:72 140.78.100.211	Spanning-tree-(for-k 140.78.100.140	ICMP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e Echo (ping) request	
18 5.151104	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
19 5.174213	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
20 6.174206 21 6.590423	e0:69:95:12:cd:15 HewlettP_c9:64:72	Broadcast Spanning-tree-(for-k	ARP	who has 140.78.100.138? Tell 140.78.100.212 RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
					_
'ame 8 (74 bytes on wi	re, 74 bytes captured)				
Arrival Time: May 18	2012 13.02.17 726145000				
	2012 13:02:17.726145000 ious captured frame: 0.001149	000 seconds]			
[Time delta from prev					
[Time delta from prev [Time delta from prev [Time since reference	ious captured frame: 0.001149	9000 seconds]			
[Time delta from prev [Time since reference Frame Number: 8	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by [Frame is marked: Fal	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se]	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame:	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data]	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name:	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP]	9000 seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byt [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String	ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP]	9000 seconds] seconds]	2d:7f (00	:13:20:e9:2d:7f)	
[Time delta from prev [Time delta from prev [Time since reference Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] tCMP] : icmp icmpv6]</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9:			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76 ternet Protocol, Src:	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] :8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9:			
[Time delta from prev [Time delta from prev [Time since reference Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String thernet II, Src: 2c:76	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] :8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9:			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76 ternet Protocol, Src:	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] :8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9:			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76 ternet Protocol, Src: ternet Control Messag	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] :8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1 e Protocol</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76 tternet Protocol, Src: tternet Control Messag	<pre>ious captured frame: 0.001149 ious displayed frame: 0.00114 or first frame: 2.160081000 s tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] :8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1 e Protocol</pre>	9000 seconds] seconds] e2), Dst: IntelCor_e9:			

Wireshark Ping

ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> naly	rection - Wireshark /ze <u>S</u> tatistics Telephon <u>y T</u> ools <u>H</u> elp							
n m g g g g 🖻 🗖	🗙 😂 占 🔍 🗢 🌳 🎝 🚡		9 🖭	a 🗹 畅 💥 💢				
ilter:	•	Expression Clear Apply						
lo Time	Source	Destination	Protocol	Info				
1 0.000000	Intel_76:be:36	Broadcast	ARP	Who has 140.78.100.141?				
2 0.174052	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138?				
3 0.579412	HewlettP_c9:64:72	Spanning-tree-(for-b		RST. Root = 32768/100/00			Port = $0x800e$	
4 0.864438	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138?				
5 0.999988	Intel_76:be:36 Intel_40:e1:0d	Broadcast Broadcast	ARP ARP	who has 140.78.100.141? who has 140.78.100.138?				
6 1.854523 7 2.158932	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	1011 140.78.100.12	9		
8 2.160081	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply				
9 2.579815	HewlettP_c9:64:72	Spanning-tree-(for-b		RST. Root = 32768/100/00	0.23.34.56.76.00 00	st = 220008	Port = $0x800e$	
10 2.854583	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138?	Tell 140, 78, 100, 12	9		
11 3.149568	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request				
12 3.150553	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply				
13 4.149606	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request				
14 4.150692	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply				
15 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138?	Tell 140.78.100.21	2		
16 4.580183	HewlettP_c9:64:72	Spanning-tree-(for-b		RST. Root = 32768/100/00	0:23:34:56:7c:00 Co	5t = 220008	Port = 0x800e	
17 5.149709	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request				
18 5.151104	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply				
19 5.174213	e0:69:95:12:cd:15	Broadcast	ARP	Who has 140.78.100.138?				
20 6.174206 21 6.590423	e0:69:95:12:cd:15 HewlettP_c9:64:72	Broadcast Spanning-tree-(for-b	ARP	<pre>who has 140.78.100.138? RST. Root = 32768/100/00</pre>			0000	
Erame 8 (74 hytes on wir	e 74 bytes cantured)							
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9	8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) :2d:7f (00:13:20:e9:2d:7f)		2d:7f (00	0:13:20:e9:2d:7f)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0	8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua	al address (unicast)	Ī					
Ethernet II, Src: 2c:76: ⊡ Destination: IntelCor_ Address: IntelCor_e9 0	8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally	al address (unicast)	Ī					
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_es 0 ■ Source: 2c:76:8a:3e:a0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) :2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2)</pre>	al address (unicast)	Ī					
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) :2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2) ::a0:e2 (2c:76:8a:3e:a0:e2)</pre>	al address (unicast) unique address (factor	Ī					
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: Intelcor_e9 0 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2) ::a0:e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua</pre>	al address (unicast) unique address (factor al address (unicast)	ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: Intelcor_e9 0 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) :2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2) ::a0:e2 (2c:76:8a:3e:a0:e2)</pre>	al address (unicast) unique address (factor al address (unicast)	ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: Intelcor_e9 0 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2) ::a0:e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua</pre>	al address (unicast) unique address (factor al address (unicast)	ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_Address: Intelcor_e9 0 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally 0:e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 ■ Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src:	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 ■ Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src:	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 ■ Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src:	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 ■ Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src:	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e .e9:2d:7f (00:13:20:e9:2d:7f) .:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally = LG bit: Globally = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_Address: IntelCor_e9 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = IG bit: Globally 0:e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: Destination: IntelCor_ Address: IntelCor_e9 0 Bource: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally :e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 : protocol 76 8a 3e a0 e2 08 00 45 00</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_Address: Intelcor_e9 0	<pre>8a:3e:a0:e2 (2::76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Globally 0:e2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 00 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 000 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21	ry defaul ry defaul	t)				
□ Destination: IntelCor_ Address: IntelCor_e9 0	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 000 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 0 0 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 00 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 00 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 00 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				
Ethernet II, Src: 2c:76: □ Destination: IntelCor_ Address: IntelCor_e9 00 Source: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e:a0 Address: 2c:76:8a:3e 0 0 Type: IP (0x0800) Internet Protocol, Src: Internet Control Message 00 00 13 20 e9 2d 7f 2c 10 00 3c 0a 5c 00 00 40 20 64 d3 00 00 55 40 00 30 67 68 69 6a 6b 6c 6d	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e e9:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) 0:2d:7f (00:13:20:e9:2d:7f) = IG bit: Individua = LG bit: Idividua = LG bit: Globally pe2 (2c:76:8a:3e:a0:e2) = IG bit: Individua = LG bit: Globally 140.78.100.140 (140.78.100.14 Protocol 76 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e 01 00 1b 61 62 63 64 65 66 e 6f 70 71 72 73 74 75 76</pre>	al address (unicast) unique address (factor al address (unicast) unique address (factor 10), Dst: 140.78.100.21 	ry defaul ry defaul	t)				

Wi	res	har	' <mark>k</mark>
		Pin	g

¥ ₩	📽 🕷 🕷 🗁 🗃	🗙 😂 占 🔍 🗢 🔶 孩		2 🖭 й	1 🗹 🍓 % 🔀	
iter:		•	Expression Clear Apply			
0	Time	Source	Destination	Protocol	Info	
	L 0.00000	Intel_76:be:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174	
	2 0.174052	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
	3 0.579412	HewlettP_c9:64:72	Spanning-tree-(for-br		RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
	1 0.864438	Intel_40:e1:0d	Broadcast	ARP	Who has 140.78.100.138? Tell 140.78.100.129	
	5 0.999988	Intel_76:be:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174	
	5 1.854523	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129	
	7 2.158932	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
	3 2.160081	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
	9 2.579815	HewlettP_c9:64:72	Spanning-tree-(for-br		RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
	2.854583	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129	
	L 3.149568	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
	2 3.150553	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
	3 4.149606	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
	4.150692	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
	5 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
	5 4.580183	HewlettP_c9:64:72	Spanning-tree-(for-br		RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
	7 5.149709	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
	3 5.151104	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
	9 5.174213	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
	0 6.174206	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
21	L 6.590423	HewlettP_c9:64:72	Spanning-tree-(for-br	STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
Ether	net II, Src: 2c:76:	e, 74 bytes captured) 8a:3e:a0:e2 (2c:76:8a:3e:a0:0 140 78 100 140 (140 78 100 14				
Ether Inter Ver Hea ∃ Dif	rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: De	40), Dst: 140.78.100.21			
Ethen Inter Ver Hea ⊕ Dif Tot Ide	net II, Src: 2c:76: net Protocol, Src: 'sion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def : (2652)	40), Dst: 140.78.100.21			
Ethen Inter Ver Hea ⊡ Dif Tot Ide ■ Fla	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service cal Length: 60 entification: 0x0a5c ags: 0x00 = Reserved bit:</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def c (2652) Not Set	40), Dst: 140.78.100.21			
Ethen Inter Ver Hea ⊡ Dif Tot Ide ■ Fla	net II, Src: 2c:76: net Protocol, Src: 'sion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def c (2652) Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea ⊕ Dif Tot Ide ■ Fla	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragment</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Det : (2652) Not Set : Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea ⊡ Dif Tot Ide C	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragment .0 = More fragments</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Det : (2652) Not Set : Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide ■ Fla 0	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragments 0 = More fragments agment offset: 0</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Det : (2652) Not Set : Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fla C	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service cal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragment .0 = More fragment agment offset: 0 me to live: 64</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Det : (2652) Not Set : Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fla C	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragments 0 = More fragments agment offset: 0</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Det : (2652) Not Set : Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea ⊡ Dif Tot Ide ■ Fla 0 0	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragment .0 = More fragments agment offset: 0 me to live: 64 btocol: ICMP (0x01)</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def c (2652) Not Set :: Not Set :: Not Set :: Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea ⊡ Dif Tot Ide ■ Fla 00	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragment 0 = More fragments agment offset: 0 me to live: 64 tocool: ICMP (0x01) ader checksum: 0x8e6</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def : (2652) Not Set :: Not Set :: Not Set :: Not Set	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fla 0	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragment 0 = More fragment agment offset: 0 me to live: 64 btocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14 s s Field: 0x00 (DSCP 0x00: Def c (2652) Not Set : Not Set : Not Set : Not Set : Not Set) [correct] 0 (140.78.100.140)	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fra C Fra Tim Pro Sou Des	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service cal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: .0 = Don't fragment .0 = More fragment .0 = More fragment one to live: 64 otocol: ICMP (0x01) ader checksum: 0x8e6 stination: 140.78.100</pre>	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e1 140.78.100.140 (140.78.100.14 es es Field: 0x00 (DSCP 0x00: Def e (2652) Not Set ex N</pre>	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fra C Fra Tim Pro Sou Des	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragment 0 = More fragment agment offset: 0 me to live: 64 btocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140</pre>	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e1 140.78.100.140 (140.78.100.14 es es Field: 0x00 (DSCP 0x00: Def e (2652) Not Set ex N</pre>	40), Dst: 140.78.100.21			
Ether Inter Ver Hea Dif Tot Ide Fra Tim Pro Sou Des Inter	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0 = Reserved bit: 0. = Don't fragment = More fragment agment offset: 0 me to live: 64 btocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140 stination: 140.78.10</pre>	<pre>8a:3e:a0:e2 (2c:76:8a:3e:a0:e 140.78.100.140 (140.78.100.14) ss ss Field: 0x00 (DSCP 0x00: Def c (2652) Not Set :: Not Set :: Not Set i9 [correct] 0 (140.78.100.140) 0.211 (140.78.100.211) : Protocol</pre>	10), Dst: 140.78.100.21			
Ether Inter Ver Hea ⊕ Dif Tot Ide ■ Fla 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragments agment offset: 0 me to live: 64 btocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140 stination: 140.78.100 tination: 140.78.100 tination: 140.78.100 oret Control Message 0 13 20 e9 2d 7f 2c 0 3c 0a 5c 00 04 04 4 d3 00 00 55 40 00 7 68 69 6a 6b 6c 6d</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e1 140.78.100.140 (140.78.100.14 is is Field: 0x00 (DSCP 0x00: Def : (2652) Not Set :: Not Set : Not Se	<pre>i0), Dst: 140.78.100.21; fault; ECN: 0x00)evebcdef ghijklmopgrstuv</pre>			
Ether Inter Ver Hea Diff Tot Ide ■ Fla 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<pre>rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service cal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragment .0 = More fragments agment offset: 0 me to live: 64 otocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140 stination: 140.78.100 rnet Control Message 0 13 20 e9 2d 7f 2c 0 3c 0a 5c 00 00 40 4 d3 00 00 55 40 00</pre>	8a:3e:a0:e2 (2c:76:8a:3e:a0:e1 140.78.100.140 (140.78.100.14 is is Field: 0x00 (DSCP 0x00: Def : (2652) Not Set :: Not Set : Not Se	i0), DST: 140.78.100.21 Fault; ECN: 0x00) E. E. E. E. E. E. E. E. E. E.			
Ether Inter Ver Hea ⊕ Dif Tot Ide ■ Fla 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	rnet II, Src: 2c:76: rnet Protocol, Src: rsion: 4 ader length: 20 byte fferentiated Service tal Length: 60 entification: 0x0a5c ags: 0x00 0. = Reserved bit: 0. = Don't fragments agment offset: 0 me to live: 64 btocol: ICMP (0x01) ader checksum: 0x8e6 urce: 140.78.100.140 stination: 140.78.100 tination: 140.78.100 140 30 00 55 40 00 7 68 69 66 56 46	8a:3e:a0:e2 (2c:76:8a:3e:a0:e1 140.78.100.140 (140.78.100.14 is is Field: 0x00 (DSCP 0x00: Def : (2652) Not Set :: Not Set : Not Se	<pre>i0), Dst: 140.78.100.21; fault; ECN: 0x00)evebcdef ghijklmopgrstuv</pre>			

Michael Sonntag

Checksum: 0x5540 [correct] Identifier: 0x0001 Sequence number: 27 (0x001b)						
Image: Server Destination Pactual State 1 0.15002 Tricle 75(b):23(15) Broadcast ARP Who Nas 140.75,100.1127 Trill 140.75,100.112 Trill 140.75,100.122 Trill 140.75,100.122 Trill 140.75,100.122 Trill 140.75,100.123 Trill 140.75,100.122 Trill 140.75,100.123 Trill 140.75,100	u au au au l 👝 🗖	yze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp				
The Source Destination Probability Info 10.000000 Intel_72:5b::36 Broadcast: AAP Who has 140.78.100.1417 Tell 140.78.100.124 20.174052 e0:99398:12:cd:15 Broadcast: AAP Who has 140.78.100.1387 Tell 140.78.100.129 220008 Port = 0x800e 40.864438 Intel_72:5b::36 Broadcast: AAP Who has 140.78.100.1387 Tell 140.78.100.129 220008 Port = 0x800e 50.99398 Intel_72:5b::36 Broadcast: AAP Who has 140.78.100.1387 Tell 140.78.100.129 220008 Port = 0x800e 51.853233 Intel_40:e1:00 Broadcast: AAP Who has 140.78.100.1387 Tell 140.78.100.129 220008 Port = 0x800e 52.855383 Intel_40:e1:00 Broadcast: AAP Who has 140.78.100.1387 Tell 140.78.100.129 220008 Port = 0x800e 52.85583 Intel_40:e1:00 Broadcast: AAP Who has 140.78.100.120 220008 Port = 0x800e 51.31.313 Hold:78.100.121 140.78.100.121 140.78.100.121 140.78.100.121 140.78.100.121 140.78.100.121 140.78.100.121 140.78.100.121 140.78.100.140 140.78.100.121 140.	📕 🖼 🐝 🐘 🗁 🔂	🗙 🛃 📇 🔍 🗢 🔿 🏹	<u>⊈</u> ⊒ ⊒ €, Q	0	🏽 🖻 🥵 🖗 📜	
10.000000 Intel_76:be:36 prodcast AAP who has 140.75.100.1412 rel1 140.75.100.174 20.174052 e0:69:95:12:d1:5 spanning-tree-(for-br STP EST. BOOL = 22008 Port = 0x800e 30.579412 mewistrp.c3:64:72 spanning-tree-(for-br STP EST. BOOL = 22008 Port = 0x800e 30.579412 mewistrp.c3:64:72 spanning-tree-(for-br STP EST. BOOL = 22008 Port = 0x800e 30.579412 mewistrp.c3:64:72 spanning-tree-(for-br STP EST. BOOL = 22008 Port = 0x800e 30.579412 mewistrp.c3:64:72 spanning-tree-(for-br STP EST. BOOL = 22008 Port = 0x800e 30.59958 intel_40:78:100.111 HON 78:100.120 Ford Asta AAP who has 140.78:100.137 Tell 140.78:100.129 7.158532 140.78:100.111 HON 78:100.101 Core Ford Oping Port Port Port Port Port Port Port Port		•	Expression Clear Apply			
2 0.174052 e016951212:dd15 Broadcast APP Who has 10.78,100.1387 Tell 140.78,100.212 0.576412 mewistp. 6216472 Broadcast APP Who has 10.78,100.1387 Tell 140.78,100.129 Trel 140.78,100.111 140.78,100.140 Trel 140.121 140.78,100.129 Total 140,78,100.111 140,78,100.140 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.140 Total 140,78,100.147 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.140 Total 140,78,100.147 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.140 Total 140,78,100.141 Total 140,78,100.147 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.140 Total 140,78,100.141 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.141 Total 140,78,100.141 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.111 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.111 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.111 140,78,100.111 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.101 Total 140,78,100.111 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.101 Total 140,78,100.111 Total 140,78,100.1387 Tell 140,78,100.129 Total 140,78,100.101 Total 140,78,100.111 Total 140,78,100.121 Total 140,78,100.101 Total 140,78,100.121 Total 140,78,100.101 Total 140,78,100.121 Total 140,78,100.101 Total 140,78,100.101 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.101 Total 140,78,100.101 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.101 Total 140,78,100.101 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.111 Total 140,78,100.101 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.111 Total 140,78,100.140 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.1387 Tell 140,78,100.122 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.140 Total 140,78,100.140 Tota	Time	Source	Destination	Protocol	Info	
3 0.579412 HewlettP_C2:64:72 Spanning-tree-(for-br STP kST, Root = 32768/100/00:2213136:7C:00 Cost = 220008 Port = 0x800e 4 0.84438 Trtel_76:bi:30 Broadcast APP who has 140.78.100.131 Trell 140.78.100.12 5 1.854523 Trtel_76:bi:30 Broadcast APP who has 140.78.100.131 Trell 140.78.100.12 5 2.579813 HewlettP_C3:64772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221313657C:00 Cost = 220008 Port = 0x800e 5 2.579813 HewlettP_C3:64772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221313567C:00 Cost = 220008 Port = 0x800e 5 2.579813 HewlettP_C3:64772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221313567C:00 Cost = 220008 Port = 0x800e 5 2.579813 HewlettP_C3:64772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221313567C:00 Cost = 220008 Port = 0x800e 11 3.139583 Trtel 140.78.100.140 140.78.100.11 CosP Echo (ping) regly 13 4.139696 140.78.100.140 140.78.100.11 CosP Echo (ping) regly 14 4.130692 140.78.100.140 140.78.100.11 CosP Echo (ping) regly 15 5.14373 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221341567C:00 Cost = 220008 Port = 0x800e 15 5.139313 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221341567C:00 Cost = 220008 Port = 0x800e 15 5.139313 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221341567C:00 Cost = 220008 Port = 0x800e 15 5.13014 140.78.100.140 140.78.100.11 CosP Echo (ping) regly 15 5.131413 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221341567C:00 Cost = 220008 Port = 0x800e 15 5.13023 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:221341567C:00 Cost = 220008 Port = 0x800e 16 5.50423 HewlettP_C3:54772 Spanning-tree-(for-br STP KST, Root = 32768/100/00:213141567C:00 Cost = 220008 Port = 0x800e 17 5.148790 1140.78.100.140 (40.78.100.140), DSt: 140.78.100.211 (40.78.100.211) 16 5.50423 HewlettP_C3:56172 Spanning-tree-(for-br STP KST, Root = 32768/100/00:213141567C:00 Cost = 220008 Port = 0x800e 16 5.50423 HewlettP_C3:56172 Spanning-tree-(for-br S						
4 0.88438 Intel_40:e1:00 Broadcast APP who has 140.78.100.137 Tel 140.78.100.139 0.89988 Intel_76:b1:56 Broadcast APP who has 140.78.100.137 Tel 140.78.100.139 7 1.53933 Intel_76:b1:56 Broadcast APP who has 140.78.100.137 Tel 140.78.100.139 7 2.53933 Intel_76:b1:56 Broadcast APP who has 140.78.100.137 Tel 140.78.100.129 7 2.53933 Intel_40:c1:00 Broadcast APP who has 140.78.100.137 Tel 140.78.100.129 9 2.53933 Intel_40:c1:00 Broadcast APP Who has 140.78.100.137 Tel 140.78.100.129 9 2.53931 HeltL_50:64:72 Spanning-tree-(for-br STP RST. R00.139 Tel 140.78.100.129 13 1.439668 140.78.100.11 140.78.100.211 Cho (pin) reguest 14 1.50692 140.78.100.10 ICMP Echo (pin) reguest 14 1.40683 Hewlettr_51:64:72 Spanning-tree-(for-br STP RST. R00.1387 Tel 140.78.100.212 14 3.13083 Hewlettr_51:64:72 Spanning-tree-(for-br STP RST. R00.1387 Tel 140.78.100.212 VERSION 140 14 3.130833 Hewlettr_51:64:7						
5 0.99986 Intel_76:be:36 Broadcast ARP who has 140.78.100.141? Tell 140.78.100.142 6 1.854533 1176E_10.61:00 Broadcast ARP who has 140.78.100.141? Tell 140.78.100.124 7 1.159371 10.78.100.211 10.78.100.211 10.78.100.141 COP ECO (ping) request 0 2.59915 Healtertp.c506:72 2756/100/00023:34156:7C:00 Cost = 220008 Port = 0x800e 10 2.654583 Intel_40:61:00 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.123 11 3.149666 140.78.100.211 140.78.100.140 ICMP ECO (ping) request 14 4.15662 140.78.100.211 140.78.100.101 ICMP ECO (ping) request 14 4.15662 140.78.100.211 140.78.100.121 ICMP ECO (ping) request 14 4.15662 140.78.100.211 140.78.100.121 ICMP ECO (ping) request 15 4.33133 e0:669:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 15 4.33134 e0:669:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 15 4.53013 Healtertp.c548:72 Spanning-tree.(for-br 5TP EST, Root = 32765:100/00:23:34156:7C:00 Cost = 220008 Port = 0x800e 15 5.174206 e0:669:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 15 5.174213 e0:69:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 15 5.174206 e0:669:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 16 5.0023 Healterp.c96:72 Spanning-tree.(for-br 5TP EST Port ECO (ping) reply 16 5.174206 e0:669:95:112:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 16 5.0023 Port = 0x800e 17 Erent Control Message Protocol 17 Erent Control Message Protocol 18 York Sourd Source 20008 Port = 0x800e 18 York Source 20008 Port = 0x800e 19 York Source 20008 Port = 0x800e York Source 20008 Port = 0x800e 19 York Source 200	4 0.864438	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129	
7 2.158932 140.78.100.211 140.78.100.140 TCVP Echo (ping) request 8 2.160001 1407.85100.140 1407.85100.141 Gtor (ping) request 9 2.559815 HeilettP.2018472 Spanning-tree.(for-br STP RST. Noot = 32785100/0012313415817:00 Cost = 220008 Port = 0x800e 9 2.559815 HeilettP.2018472 Spanning-tree.(for-br STP RST. Noot = 32785100/0012313415817:00 Cost = 220008 Port = 0x800e 13.149585 140.78.100.211 140.78.100.211 Cost = 20008 Port = 0x800e 13.149585 140.78.100.120 140.78.100.140 CVP Echo (ping) request 13.149586 140.78.100.211 140.78.100.211 Cost = 20008 Port = 0x800e 14.150692 140.78.100.211 140.78.100.121 CVP Echo (ping) request 15.15104 140.78.100.211 140.78.100.121 CVP Echo (ping) request 15.15104 140.78.100.140 CVP Echo (ping) request 140.78.100.212 15.15104 140.78.100.140 CVP Echo (ping) request 140.78.100.212 15.15104 140.78.100.140 140.78.100.180 Echo (ping) request 140.78.100.212	5 0.999988	Intel_76:be:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174	
8 2.100031 140.78.100.211 140.78.100.211 140.78.100.211 140.78.100.211 140.78.100.113 9 2.579815 HewlettP.c9:8472 Spanning-tree(for-br 5TF RST. Root = 32768/100/00:23134:56:7C:00 Cost = 220008 Port = 0x800e 10 2.854838 Intel_40:12:00 Broadcast ARP Whe has 140.78.100.1387 Tell 140.78.100.129 Tell 140.78.100.129 11 3.150553 140.78.100.211 140.78.100.211 140.78.100.110 TCMP Echo (ping) regivest 14.150692 140.78.100.111 140.78.100.211 CMP Echo (ping) regivest 14.150692 140.78.100.211 140.78.100.211 CMP Echo (ping) regivest 14.150692 140.78.100.211 140.78.100.140 TCMP Echo (ping) regivest 15.139709 140.78.100.211 140.78.100.140 TCMP Echo (ping) regivest 15.149709 140.78.100.211 140.78.100.140 TCMP Echo (ping) regivest 15.14206 e0:09:95:12:cd:15 Broadcast ARP Who has 140.78.100.1387 Tell 140.78.100.212 15.17206 e0:09:95:12:cd:15 Broadcast ARP Who has 140.78.100.210.021 Tell 140.78.100.212						
9 2.79815 HewlettP_c3:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:2313436:7C:00 Cost = 220008 Port = 0x800e 11 3.149568 140.78.100.211 140.78.100.140 ICMP Echo (ping) request 13 1.149568 140.78.100.211 140.78.100.140 ICMP Echo (ping) request 13 1.149568 140.78.100.211 140.78.100.140 ICMP Echo (ping) request 14 1.150692 140.78.100.211 140.78.100.140 ICMP Echo (ping) request 14 1.150692 140.78.100.211 I40.78.100.140 ICMP Echo (ping) request 15 4.530183 HewlettP_c3:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23143:56:7C:00 Cost = 220008 Port = 0x800e 15 4.530183 HewlettP_c3:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23143:56:7C:00 Cost = 220008 Port = 0x800e 15 4.530183 HewlettP_c3:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:2314:56:7C:00 Cost = 220008 Port = 0x800e 16 5.530243 HewlettP_c3:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:2314:56:7C:00 Cost = 220008 Port = 0x800e 17 5 6 5 5 5 4 2 2 0 5 0 0 2 2 0 5 0 0 2 2 0 5 0 0						
10 2.854583 Intel_40:e1:0d Broadcast ARP Who has 140.78.100.137 Tell 140.78.100.129 11 3.149565 11 40.78.100.211 140.78.100.211 ICMP Echo (ping) reply Echo (ping) reply 12 3.150533 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 13 4.150652 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 14 4.150652 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 15 4.331539 e0:69:95:12:cd:15 Broadcast ARP Who has 140.78.100.137 Tell 140.78.100.212 153.157.100 Cost = 22000 Port = 0x800e 15 5.149709 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 15 6.151104 140.78.100.121 140.78.100.211 CMP Echo (ping) reply 15 6.151104 140.78.100.121 IA0.78.100.211 ICMP Echo (ping) reply 20 6.174206 e0:69:95:12:cd:15 Broadcast ARP Who has 140.78.100.137 Tell 140.78.100.212 153.151104 140.78.100.211 IA0.78.100.211 ICMP Echo (ping) reply 20 6.174206 e0:69:95:12:cd:15 Broadcast ARP Who has 140.78.100.137 Tell 140.78.100.212 12 20 6.174206 e0:69:95:12:cd:15 Broadcast ARP Who has 140.78.100.1387 Tell 140.78.100.212 12 20 6.174206 e0:69:95:12:cd:15 Broadcast ARP Who has 140.78.100.1387 Tell 140.78.100.212 12 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 20008 Port = 0x800e 21 6.590423 HewlettP_C9:64:75 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 20008 Port = 0x800e 21 6.590423 HewlettP_C9:64:56 Spanning-tree-(for-br STP RST. Root = 32768		HewlettP c9:64:72	Spanning-tree-(for-		RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
12 3.150533 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 14 4.150662 140.78.100.140 140.78.100.114 ICMP Echo (ping) reply 14 4.150662 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 14 4.150662 140.78.100.140 140.78.100.110 ICMP Echo (ping) reply 15 3.15104 140.78.100.211 ICMP Echo (ping) reply ICMP (ping) reply 15 3.15104 140.78.100.140 140.78.100.211 ICMP (ping) reply 15 3.15104 140.78.100.140 140.78.100.211 ICMP (ping) reply 15 3.15104 140.78.100.140 140.78.100.211 ICMP (ping) reply 15 3.15104 140.78.100.211 ICMP (ping) reply ICMP (ping) reply 15 3.15104 140.78.100.211 ICMP (ping) reply ICMP (ping) reply 15 3.15104 140.78.100.211 ICMP (ping) reply ICMP (ping) reply 15 3.15104 140.78.100.211 ICMP (ping) reply ICMP (ping) reply 15 3.152105 Broadcast ARP Wo has 140.78.100.1387 rell 140.78.100.212 ICMP (ping) reply 15 6.154206 Ceito (ping) reply <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
13 4.149606 140.78.100.211 140.78.100.211 1CXP Echo (ping) request 14 4.150692 140.78.100.140 140.78.100.211 1CXP Echo (ping) request 15 4.331539 e0:69:95:12:tcd:15 Broadcast APP Who has 140.78.100.1387 Tell 140.78.100.212 (140.78.100.212) 16 4.580183 HewlettP.c9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:45:57:t00 Cost = 220008 Port = 0x800e 15 5.151104 140.78.100.211 140.78.100.211 140.78.100.211 CMP Echo (ping) request 15 5.151104 140.78.100.212 error of the state of the sta						
14 4.150692 140.78.100.140 140.78.100.211 ICMP Echo (ping) reply 15 4.331539 e0:69:99:1212:d15 Broadcast ARP Who has 140.78.100.1387 rell 140.78.100.212 Spanning-tree-(for-br STP K5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 15 5.145709 140.78.100.140 140.78.100.141 ICMP Echo (ping) request 15 5.145709 140.78.100.211 IA0.78.100.141 ICMP Echo (ping) request 15 5.145709 140.78.100.212 Spanning-tree-(for-br STP K5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 15 5.174206 e0:69:95:12:d15 Broadcast ARP Who has 140.78.100.1387 rell 140.78.100.212 Spanning-tree-(for-br STP K5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 16 6.590423 HewlettP_c9:66:72 Spanning-tree-(for-br STP K5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 16 6.590423 HewlettP_c9:60:72 Spanning-tree-(for-br STP K5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 16 6.590423 HewlettP_c9:00 Lot 0.58:00.140 Lot 78.100.211 (140.78.100.211 (140.78.100.211) 16 6.590423 HewlettP_c9:20:7f:63a:3e:a0:e2), Dst: IntelCor_e9:20:7f (00:13:20:e9:2d:7f) rernet Protocol, src: 140.78.100.140, bst: 140.78.100.211 (140.78.100.211) 16 execusin: 0x5540 [correct] 16 develop reply 16 develop reply 16 develop reply 16 develop fing) reply 17 develop reply 16 develop fing) reply 17 develop reply 16 develop fing reply 16 develop fing reply 17 develop fing reply 18 develop fing						
15 4.333539 e0:69:95:12:cd:15 Broadcast APP who has 140.78.100.1387 Tell 140.78.100.212 Spanning-tree-(for-for STP RST. Root = 32768/100/0023134156:72:00 Cost = 220008 Port = 0x800e 16 4.38013 HewlettP_c0:61.21 140.78.100.140 ICMP Echo (ping) request 18 1.51104 140.78.100.211 140.78.100.140 ICMP Echo (ping) request 18 1.51104 140.78.100.111 ICMP Echo (ping) request 18 1.51104 140.78.100.121 Broadcast APP who has 140.78.100.1387 Tell 140.78.100.212 18 1.51104 140.78.100.111 ICMP Echo (ping) request ICMP Echo (ping) request 18 1.51104 140.78.100.111 ICMP Echo (ping) request ICMP Echo (ping) request 18 1.51104 140.78.100.121 ICMP Echo (ping) reply ICMP Echo (ping) reply 16 1.5004 e0:69:511:10:60:61:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:70:00 Cost = 220008 Port = 0x800e mme 8 (74 bytes on wire, 74 bytes captured) ernet II, src: 27:61:83:92:a0:e2 Echo (ping) reply Ec		140.78.100.211	140.78.100.140		Echo (ping) request	
16 4.580183 HewlettP_c9:64:72 Spanning-tree-(for-br STP R5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e 17 5.149709 140.78.100.110 140.78.100.211 I40.78.100.211 ICMP ECho (ping) reguest 18 5.151104 140.78.100.140 140.78.100.211 IGMP ECho (ping) reguest 19 5.174213 e0:669:95:12:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 20 6.174206 e0:68:95:12:cd:15 Broadcast ARP who has 140.78.100.1387 Tell 140.78.100.212 21 6.590423 HewlettP_c9:46:72 Spanning-tree-(for-br STP R5T. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e me 8 (74 bytes on wire, 74 bytes captured) mernet T1, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f) rernet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211) rernet Control Message Protocol ype: 0 (cho (ping) reply) code: 0 () checksum: 0x5540 [correct] identifier: 0x0001 iequence number: 27 (0x01b) ata: 01526564656666666666666666666666666666666		e0:69:95:12:cd:15				- V
18 5.151104 140.78.100.140 140.78.100.211 ICP ECHO (ping) reply 19 5.174213 e0:69:95:12:cd:15 Broadcast ARP who has 140.78.100.1387 rell 140.78.100.212 20 6.174206 e0:69:95:12:cd:15 Broadcast ARP who has 140.78.100.1387 rell 140.78.100.212 140.78.100.1387 rell 140.78.100.212 20008 Port = 0x800e meme 8 (74 bytes on wire, 74 bytes captured) mernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: Intelcor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Onlow Series Protocol repret 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211) repret Onlow Series Protocol repret Octoo (ping) reply) code: 0 () checksum: 0x5540 [correct] tedentifier: 0x0001 sequence number: 27 (0x001b) Data: 61626464566666668696666666666666666666666666	16 4.580183		Spanning-tree-(for-	br STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
19 5.1/4213 e0:69:95:12:cd:15 Broadcast APP who has 140.78.100.138? Tell 140.78.100.212 20 6.174206 e0:69:95:12:cd:15 Broadcast APP who has 140.78.100.38? Tell 140.78.100.212 21 6.590423 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7C:00 Cost = 220008 Port = 0x800e me 8 (74 bytes on wire, 74 bytes captured) mernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), bst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Protocol, Src: 140.78.100.140 (140.78.100.140), bst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol type: 0 (ccho (ping) reply) code: 0 () thecksum: 0x5540 [correct] tequence number: 27 (0x001b) Data: 6102636465666768696A6B6C6D6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00 (V.>E.						
20 6.174206 e0:69:95:12:cd:15 Broadcast APP Who has 140.78.100.1387 Tell 140.78.100.212 HewlettP_C9:64:72 Spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e me 8 (74 bytes on wire, 74 bytes captured) hernet II, Src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), Dst: IntelCor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol rype: 0 (Echo (ping) reply) code: 0 () thecksum: 0x5540 [correct] tedentifier: 0x0001 Sequence number: 27 (0x001b) Jata (32 bytes) Data: 612636465566676869664686C6066667707172737475767761 [Length: 32]					ECNO (ping) reply who has 140 78 100 1282 moll 140 78 100 212	
21 6.590423 HewlettP_C9:64:72 spanning-tree-(for-br STP RST. Root = 32768/100/00:23:34:56:7C:00 Cost = 220008 Port = 0x800e ame 8 (74 bytes on wire, 74 bytes captured) Image: Cost = C						
<pre>hernet II, src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), bst: Intelcor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Protocol, src: 140.78.100.140 (140.78.100.140), bst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol type: 0 (Echo (ping) reply) tode: 0 () thecksum: 0x5540 [correct] tdentifier: 0x0001 sequence number: 27 (0x001b) bata (32 bytes) Data: 626364645666768696A6866C6b6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,,V .>E. 00 3c 0a 5c 00 00 dv 01 8e 66 8 r. de 64 8r 8c 4e < \ A i ind N </pre>	21 6.590423	HewlettP_c9:64:72	Spanning-tree-(for-	br STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
<pre>hernet II, src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), bst: Intelcor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Protocol, src: 140.78.100.140 (140.78.100.140), bst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol type: 0 (Echo (ping) reply) tode: 0 () thecksum: 0x5540 [correct] tdentifier: 0x0001 sequence number: 27 (0x001b) bata (32 bytes) Data: 626364645666768696A6866C6b6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,,V .>E. 00 3c 0a 5c 00 00 dv 01 8e 66 8 r. de 64 8r 8c 4e < \ A i ind N </pre>						
<pre>hernet II, src: 2c:76:8a:3e:a0:e2 (2c:76:8a:3e:a0:e2), bst: Intelcor_e9:2d:7f (00:13:20:e9:2d:7f) ternet Protocol, src: 140.78.100.140 (140.78.100.140), bst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol type: 0 (Echo (ping) reply) tode: 0 () thecksum: 0x5540 [correct] tdentifier: 0x0001 sequence number: 27 (0x001b) bata (32 bytes) Data: 626364645666768696A6866C6b6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,,V .>E. 00 3c 0a 5c 00 00 dv 01 8e 66 8 r. de 64 8r 8c 4e < \ A i ind N </pre>						v
<pre>ternet Protocol, Src: 140.78.100.140 (140.78.100.140), Dst: 140.78.100.211 (140.78.100.211) ternet Control Message Protocol Type: 0 (Echo (ping) reply) tode: 0 () thecksum: 0x5540 [correct] tdentifier: 0x0001 sequence number: 27 (0x001b) tata (32 bytes) Data: 6162636465666768696A68666b6e6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,, V. >, E. 00 3c 0a 5c 00 004 001 8e 68 8c 4e 64 8c 8c 4e, V. >, E. 00 3c 0a 5c 00 004 001 ternet sequence ternet ternet.</pre>	ame 8 (74 bytes on wi	re, 74 bytes captured)				
cernet Control Message Protocol type: 0 (Echo (ping) reply) code: 0 () thecksum: 0x5540 [correct] tdentifier: 0x0001 sequence number: 27 (0x001b) tata (32 bytes) Data: 61626364656667688696A6B6C6b6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00 E. 00 3r 0a 5c 00 00 40 01 8e 69 8c 4e 6d 8c 8c 4e ed. E.						
rype: 0 (Echo (ping) reply) code: 0 () :hecksum: 0x5540 [correct] identifier: 0x0001 Sequence number: 27 (0x001b) bata (32 bytes) Data: 6162636465666768696A6B6C6D6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00 ,ve. 00 37 0a 5c 00 00 40 01 8e 69 8c 4e 6d 8c 8c 4e , VE.			40), Dst: 140.78.100.7	211 (140.78	3.100.211)	
Ode: 0 ()						
00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00 v 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4e E.		reply)				
00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00 v 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4e E.						
Sequence number: 27 (0x001b) Data: (32 bytes) Data: 6162636465666768696A6B6C6D6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,V .>E. 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4eV .>E.	Code: 0 ()					
Data: (32 bytes) Data: 6162636465666768696A6B6C6D6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00v .>E. 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4ev .>E.	code: 0 () Checksum: 0x5540 [corr	rect]				
Data: 6162636465666768696A6B6C6D6E6F707172737475767761 [Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00V .>E. 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4eV .>E.	Code: 0 () Checksum: 0x5540 [corn Identifier: 0x0001	-				
[Length: 32] 00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00,V .>E. 00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4eVE.	code: 0 () Checksum: 0x5540 [corn Identifier: 0x0001 Sequence number: 27 (0	-				
00 13 20 e9 2d 7f 2c 76 8a 3e a0 e2 08 00 45 00, v .>E.	code: 0 () checksum: 0x5540 [corn dentifier: 0x0001 sequence number: 27 (Data (32 bytes)	0x001b)	107701			
$00.3c$ $0a.5c$ $00.00.40.01$ $8e.69.8c$ $4e.64.8c$ $8c$ $4e. < \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	code: 0 () checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761			
$00.3c$ $0a.5c$ $00.00.40.01$ $8e.69.8c$ $4e.64.8c$ $8c$ $4e. < \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	code: 0 () checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761	_		
$00.3c$ $0a.5c$ $00.00.40.01$ $8e.69.8c$ $4e.64.8c$ $8c$ $4e. < \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	code: 0 () checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761	-		
$00.3c$ 0a 5c 00.00 40.01 8e 69.8c 4e 64.8c 8c 4e $< \sqrt{6}$ ind N	code: 0 () hecksum: 0x5540 [corr dentifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761	-		
$00.3c$ 0a 5c 00.00 40.01 8e 69.8c 4e 64.8c 8c 4e $< \sqrt{6}$ ind N	code: 0 () hecksum: 0x5540 [corr dentifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761			
$00.3c$ $0a.5c$ $00.00.40.01$ $8e.69.8c$ $4e.64.8c$ $8c$ $4e. < \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	code: 0 () checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761			
$00.3c$ $0a.5c$ $00.00.40.01$ $8e.69.8c$ $4e.64.8c$ $8c.4e. < \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	code: 0 () hecksum: 0x5540 [corr identifier: 0x0001 Sequence number: 27 (4 oata (32 bytes) Data: 61626364656666	0x001b)	767761			
$00.3c$ 0a 5c 00.00 40.01 8e 69.8c 4e 64.8c 8c 4e $< \sqrt{6}$ ind N	code: 0 () hecksum: 0x5540 [corr dentifier: 0x0001 Sequence number: 27 (4 Data (32 bytes) Data: 6162636465666	0x001b)	767761			
00 3c 0a 5c 00 00 40 01 8e 69 8c 4e 64 8c 8c 4e < \ @ i Nd N	code: 0 () hecksum: 0x5540 [corr identifier: 0x0001 Sequence number: 27 (4 oata (32 bytes) Data: 61626364656666	0x001b)	767761			
64 65 66 67 68 69 64 65 66 67 68 69 77 61 62 63 64 65 66 67 68 69 wabcdefg hi	Code: 0 () hecksum: 0x5540 [corn identifier: 0x0001 sequence number: 27 (f bata (32 bytes) Data: 61626364656666 [Length: 32] 00 13 20 e9 2d 7f 2c	0x001b) 768696A6B6C6D6E6F707172737475 76 8a 3e a0 e2 08 00 45 00	E.			
77 61 62 63 64 65 66 67 68 69 wabcdefg hi	Code: 0 () Checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (f Data (32 bytes) Data: 6162636465666 [Length: 32]	0x001b) 768696A6B6C6D6E6F707172737475 768 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e	,V.>E. .<.\.@i.NdN			
	Code: 0 () Checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (f Data: 6162636465666 [Length: 32] 00 13 20 e9 2d 7f 2c 00 3c 0a 5c 00 00 40	0x001b) 768696A6B6C6D6E6F707172737475 768 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e	E. .<.\@1.NdN dU@ECCET			
	Code: 0 () hecksum: 0x5540 [corr identifier: 0x0001 sequence number: 27 (i bata (32 bytes) Data: 6162636465666 [Length: 32] 00 13 20 e9 2d 7f 2c 00 3c 0a 5c 00 00 40	0x001b) 768696A6B6C6D6E6F707172737475 768 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e	E. .<.\.@abcdef dh.ikim.opgrstuv			
	Code: 0 () Checksum: 0x5540 [corr Identifier: 0x0001 Sequence number: 27 (f Data: 6162636465666 [Length: 32] 00 13 20 e9 2d 7f 2c 00 3c 0a 5c 00 00 40	0x001b) 768696A6B6C6D6E6F707172737475 768 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e	E. .<.\.@abcdef dh.ikim.opgrstuv			
	00de: 0 () hecksum: 0x5540 [corrider: 0x0001 identifier: 0x0001 isequence number: 27 (interpretation of the sequence of t	0x001b) 768696A6B6C6D6E6F707172737475 768 8a 3e a0 e2 08 00 45 00 01 8e 69 8c 4e 64 8c 8c 4e	E. .<.\.@abcdef dh.ikim.opgrstuv			

Wireshark HTTP - DNS

-OX

F	
	📶 Intel(R) PRO/100 VE Network Connection - Wireshark

Eile	Edit	View	Go	Capture	<u>A</u> nalyze	Statistics	Telephony	Tools	Help	
------	------	------	----	---------	-----------------	------------	-----------	-------	------	--

Filter:	•	Expression Clear_ Apply		
No Time	Source	Destination	Protocol	Info
/ 1.69868/	/4.125.232.239	140.78.100.211	TCP	nttps > 8462 [ACK] Seq=1 ACK=2 W1N=257 Len=0 SLE=1 SRE=2
8 1.750405	140.78.100.211	140.78.100.119	DNS	Standard query A www.bing.at
9 2.034608	140.78.100.119	140.78.100.211	DNS	Standard query response A 65.52.107.149
10 2.035153	140.78.100.211	140.78.100.119	DNS	Standard query AAAA www.bing.at
11 2.315500	140.78.100.119	140.78.100.211	DNS	Standard query response
12 2.316318	140.78.100.211	65.52.107.149	TCP	8644 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8
13 2.316646	140.78.100.211	65.52.107.149	TCP	8645 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8
14 2.436395	65.52.107.149	140.78.100.211	TCP	http > 8644 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0
15 2.436499	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] seq=1 Ack=1 win=65536 Len=0
16 2.436609	65.52.107.149	140.78.100.211	TCP	http > 8645 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0
17 2.436639	140.78.100.211	65.52.107.149	TCP	8645 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
18 2.437177	140.78.100.211	65.52.107.149	HTTP	GET / HTTP/1.1
19 2.603541	65.52.107.149	140.78.100.211	HTTP	HTTP/1.1 301 Moved Permanently
20 2.609521	140.78.100.211	140.78.100.119	DNS	Standard query A www.bing.com
21 2.791682	Intel_40:e1:0d	Broadcast	ARP	Who has 140.78.100.141? Tell 140.78.100.129
22 2.791711	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129
23 2.807614	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] Seq=396 Ack=302 win=65280 Len=0
24 2.986566	140.78.100.119	140.78.100.211	DNS	Standard query response CNAME akam.bing.com CNAME a134.lm.akamai.net A 193.17
25 2.987423	140.78.100.211	140.78.100.119	DNS	Standard query AAAA www.bing.com
26 2.992487	140.78.100.119	140.78.100.211	DNS	Standard query response CNAME akam.bing.com CNAME a134.lm.akamai.net
27 2.993391	140.78.100.211	193.170.140.71	TCP	8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8
28 2.993682	140.78.100.211	193.170.140.71	TCP	8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8
29 2.996685	193.170.140.71	140.78.100.211	TCP	http > 8648 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 WS=2
30 2.996742	140.78.100.211	193.170.140.71	TCP	8648 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
▪ Frame 8 (71 bytes on wire				
Ethernet II, Src: IntelCo	r_e9:2d:7f (00:13:20:e9:2d:	7f), Dst: Intel_40:e1	L:0d (00:07	:e9:40:e1:0d)
Internet Protocol, Src: 14				
		Port, domain (55)		
🗆 Domain Name System (query)			
[Response In: 9]				
Transaction ID: 0x005f				
	auerv)			
Ouestions: 1	4 77			
Answer RRs: 0				
Authority RRs: 0				
Additional RRs: 0				
🗖 Queries				
www.bing.at: type A,	class IN			
Name: www.bing.at				
Type: A (Host addre	ss)			
Class: IN (0x0001)				
1				
1				

0000 00 07 e9 40 e1 0d 00 13 20 0010 00 39 2b 6b 00 00 13 20 0020 64 77 d3 f6 03 30 25 94 0030 00 00 00 00 00 03 77 77 0040 61 74 00 00 01 00 01	fb 00 5f 01 00 00 01	@E. .9+kb.Nd.N dw5.% w ww.bing. at	
Text item (), 17 bytes	Packets: 346 Displayed: 346 Marked:	0 Dropped: 0	Profile: Default

Wireshark **HTTP - DNS**

25 2.987423 140.78.100.211 140.78.100.119 DNS Standard query AAAA www.bing.com			₮ 坐 ■ ■ ● २	0	🏽 🗹 🎭 🖗 🕱
1.1:098087 1/4.1/2.7:227:23 1407.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 000.55:210/2149 5tandard query response X 05:52:10/2149 11.2:2:312313 110.7:8:100.211 107.78:100.211 000.211 107.78:100.211 000.55:107:149 5tandard query response X 05:52:100.149 12:2:312313 110.7:8:100.211 65:52:107:149 100.211 100.78:100.211 65:52:107:149 100.78:100.211 65:52:107:149 100.78:100.211 65:52:107:149 100.78:100.211 65:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 60:52:107:149 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100.78:100.211 100:170:100:11	Filter:		▼ Expression Clear Apply		
8 1.750405 140.78.100.211 140.78.100.211 0X5 Standard query A www.bing.at 9 2.035430 140.78.100.211 140.78.100.119 DNS Standard query A www.bing.at 110 2.035133 140.78.100.211 140.78.100.119 DNS Standard query A www.bing.at 111 2.31500 140.78.100.211 0X5 Standard query A www.bing.at 111 2.31500 140.78.100.211 0X5 Standard query A www.bing.at 112 2.315446 140.78.100.211 0X5 Standard query A www.bing.at 112 2.315446 140.78.100.211 0X5 Standard query A www.bing.at 112 2.315445 140.78.100.211 0X5.2107.149 TCP Note: Standard query A www.bing.at 12 2.436499 140.78.100.211 65.52.107.149 TCP Nthr > 8645 > http [AT Nthr > 8545 Standard query A www.bing.at 12 2.436639 140.78.100.211 65.52.107.149 TCP Nthr > 8645 > http [AT Nthr > 8645 Standard query A www.bing.at 12 2.73162 107.78.100.211 65.52.107.149 TCP Nthr > 8645 Standard query A www.bing.at 12 2.73162 107.18 140.78.100.211 Nthr > 8645 > http [XT] Nthr > 8645 > http [XT] Nthr >					
9 2203600 100 78.100.211 140.78.100.211 DNS Standard query response in 65.52.107.139 11 2.315500 140.78.100.211 65.52.107.149 TCP 8644 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.315616 140.78.100.211 65.52.107.149 TCP 8644 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.315616 140.78.100.211 65.52.107.149 TCP 8644 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.316616 140.78.100.211 TCP 8645 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.316629 65.52.107.149 140.78.100.211 TCP 8645 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.436639 16.52.107.149 140.78.100.211 TCP 8645 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.436639 16.52.107.149 140.78.100.211 TCP 8645 > http [SN] Seq=0 win=8175 tem=0 MSS=1460 WS=8 12 2.436639 16.52.107.149 140.78.100.211 TCP 8645 > http [SN] MSG=0 win MSS=1460 WS=8 12 2.436639 16.52.107.149 140.78.100.211 HTP HTP/1.1 Note: Second WSS=1460 WS=8 22 2.791711 Treel_40*8:100.211 65.52.107.149 TWO MSS Standard query MSS Note: Second WSS=1460 WS=8<		/4.125.232.239			nttps > 8462 [ACK] Seq=1 ACK=2 W1n=257 Len=0 SLE=1 SRE=2 Standard guery A www.bing.at
10 2.035133 140.78.100.211 140.78.100.211 DNS Standard guery AxAA www.bing.at 11 2.315500 140.78.100.211 65.52.107.149 TCP 8644 > http [SvN] seq-0 win-8132 Leno MSS-1460 wS-8 13 2.316646 140.78.100.211 65.52.107.149 TCP 8644 > http [SvN] seq-0 win-8132 Leno MSS-1460 wS-8 14 2.436395 65.52.107.149 140.78.100.211 TCP 8644 > http [SvN] seq-0 win-8132 Leno MSS-1460 wS-8 15 2.436499 140.78.100.211 65.52.107.149 TCP 8644 > http [SvN] seq-0 win-8132 Leno MSS-1460 wS-8 16 2.435699 65.52.107.149 140.78.100.211 TCP 8644 > http [SvN] seq-0 win-8132 Leno MSS-1460 wS-8 17 2.436699 65.52.107.149 140.78.100.211 TCP 8644 > http [Addition MSS-1460 wS-8 18 2.43727 140.78.100.211 HTP HTP HTP Match Standard guery response CNME akam.bing.com CNME al34.1m. akam 20 2.603541 60521 140.78.100.211 Broadcast ARP who has 140.78.100 21 2.791682 Intel_40:e1:00 Broadcast ARP who has 140.78.100 Now.bing.at 22 2.997423 140.78.100.211 DNS Standard guery response CNME akam.bing.com CNME al34.1m. akam					
12 2.316318 140.78.100.211 65.52.107.149 TCP 8644 > http [SVN] Seq=0 Win=8195_en=0 MSS=1460 WS=8 14 2.436393 65.52.107.149 140.78.100.211 65.52.107.149 TCP 8645 > http [SVN] Seq=0 Win=8195_en=0 MSS=1460 WS=8 14 2.436393 65.52.107.149 140.78.100.211 65.52.107.149 TCP 8645 > http [SVN] Seq=0 Win=8195_en=0 MSS=1460 WS=8 14 2.436493 140.78.100.211 65.52.107.149 TCP 8644 > http [SVN] Seq=0 Win=8195_en=0 MSS=1460 WS=8 18 2.437177 140.78.100.211 65.52.107.149 TCP 8644 > http [AV Mbat's this? Investigate 20 2.609511 140.78.100.211 65.52.107.149 TTP REM 4 > http [AV Note: Google Chrome U 21 2.791682 1ntel_40:e1:0d Broadcast APP Who has 140.78.100 Note: Google Chrome U 24 2.98656 140.78.100.119 140.78.100.119 DNS Standard query response CNAVE akam.bing.com CNAVE	10 2.035153	140.78.100.211	140.78.100.119	DNS	Standard query AAAA www.bing.at
14 2.436395 65.52.107.149 140.78.100.211 65.52.107.149 TCP http > 8644 shttp [AC] 16 2.436609 65.52.107.149 140.78.100.211 65.52.107.149 TCP http > 8645 shttp [AC] 18 2.436609 65.52.107.149 TCP 8645 shttp [AC] What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TCP 8645 shttp [AC] What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TCP http > 8645 shttp [AC] What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TCP http > 8645 shttp [AC] What's this? Investigate 21 2.79162 Intel_40:e1:0d Broadcast ARP Who has 140.78. More as 140.78.100.211 More as 140.78.100.211 Investigate 22 2.99171 Intel_40:e1:0d Broadcast ARP Who has 140.78.100.211 Investigate	11 2.315500		140.78.100.211		Standard query response
14 2.436395 65.52.107.149 140.78.100.211 65.52.107.149 TCP http > 8644 http / 8649 15 2.436639 160.78.100.211 65.52.107.149 TCP 8644 http / 8645 What's this? Investigate 18 2.436639 140.78.100.211 65.52.107.149 TCP 8645 http / 8655 What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TCP 8645 http / 865 What's this? Investigate 20 2.609321 140.78.100.211 140.78.100.211 HTTP / 140.78.100.211 HTTP / 1.301.Mg Note: Google Chrome u 21 2.79171 Intel_40:e1:0d Broadcast ARP Who has 140.78. Note: Google Chrome u 22 2.79171 Intel_40:e1:0d Broadcast ARP Who has 140.78. Note: Google Chrome u 23 2.807614 140.78.100.211 140.78.100.111 DNS Standard query response CNAME akam.bing.com Ina.kam 22 2.79171 Intel_40:e1:0d Broadcast ARP Who has 140.78. Note: Google Chrome u 23 2.807614 140.78.100.211 140.78.100.211 DNS Standard query response CNAME akam.bing.com Ina.kam 24 2.986561 140.78.100.211					8644 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
15 2.436499 140.78.100.211 65.52.107.149 140.78.100.211 TCP 8644 > http [Act 15 2.436639 140.78.100.211 65.52.107.149 HTTP \$ 8645 [S] What's this? Investigate 15 2.436639 140.78.100.211 65.52.107.149 HTTP \$ 8645 [S] What's this? Investigate 15 2.436639 140.78.100.211 65.52.107.149 HTTP \$ 8645 [S] What's this? Investigate 15 2.436639 140.78.100.211 140.78.100.119 DNS Standard query Note: Google Chrome U 22 5.93743 140.78.100.211 140.78.100.119 DNS Standard query response CNME akan.bing.com Note: Google Chrome U 23 2.93743 140.78.100.119 140.78.100.119 DNS Standard query response CNME akan.bing.com Note: Google Chrome U 24 2.98666 140.78.100.119 140.78.100.119 DNS Standard query response CNME akan.bing.com Note: Moss_1460 NS=8 25 2.99743 140.78.100.211 193.170.140.71 TCP 8648 > http [SV] Seq.0 win-8192 Len-0 MS=1460 NS=8 28 2.993682 140.78.100.211 193.170.140.71 TCP 8648 > http [SV] Seq.0 win-8192 Len-0 MS=1460 NS=8 29 2.996685 193.170.140.71<		140.78.100.211 65 52 107 149			6040 > 11CP [SYN] Seq=0 W1R=8192 Lenev MSS=1400 WS=8 http > 8644 [SYN ACK] Seq=0 Ack=1 Win=280 Lenev MSS=1460 WS=0
16 2.436609 65.52.107.149 140.78.100.211 TC P http > 8645 [St] What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TT P REF / HTTP / 1.1 What's this? Investigate 18 2.437177 140.78.100.211 65.52.107.149 TT P HTTP REF / HTTP / 1.1 Note: Socogle Chrome U 21 2.79162 111 140.78.100.211 40.78.100.211 Ansato Ansato Note: Google Chrome U 22 2.79171 Intel 40:e1:0d Broadcast ARP who has 140.78. Note: Google Chrome U 23 2.807614 140.78.100.211 95.52.107.149 TCP 8644 http [AC. Note: Google Chrome U 24 2.96566 140.78.100.211 140.78.100.211 DNS Standard query response CNAME akam.bing.com CNAME al34. lm. akam 25 2.90741 140.78.100.211 140.78.100.211 DNS Standard query response CNAME akam.bing.com CNAME al34. lm. akam 26 2.906427 140.78.100.211 140.78.100.211 DNS Standard query response CNAME akam.bing.com CNAME al34. lm. akam 26 2.906427 140.78.100.211 193.170.140.71 TCP 8644 per See Wee See Wee See Wee See Wee See Wee See S					8644 > http
19 2.603541 65.52.107.149 140.78.100.211 HTTP HTTP/1.1 301 MC 20 2.609521 140.78.100.211 140.78.100.119 DNS Standard guery Note: Google Chrome U 21 2.791682 Intel_40:e1:0d Broadcast APP who has 140.78. Note: Google Chrome U 21 2.791682 Intel_40:e1:0d Broadcast APP who has 140.78. Note: Google Chrome U 24 2.986566 140.78.100.211 40.78.100.211 Not 78.100.211 Not 7					$http > 8645$ [5] \//bat\a thia? Towart ant
19 2.603541 65.52.107.149 140.78.100.211 HTTP HTTP/1.1 301 MC 20 2.609521 140.78.100.211 140.78.100.119 DNS Standard query Note: Google Chrome U 21 2.791682 Intel_40:e1:0d Broadcast ARP who has 140.78. Note: Google Chrome U 22 2.791711 Intel_40:e1:0d Broadcast ARP who has 140.78. Note: Google Chrome U 24 2.986566 140.78.100.211 40.78.100.211 DNS Standard query response CNAME akam.bing.com CNAME al34. Im. akam 25 2.987423 140.78.100.211 140.78.100.211 DNS Standard query response CNAME akam.bing.com CNAME al34. Im. akam 27 2.993391 140.78.100.211 193.170.140.71 TCP 8644 > http [StN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.99665 193.170.140.71 140.78.100.211 TCP 8644 > http [StN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.99665 193.170.140.71 140.78.100.211 TCP 8644 > http [StN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.99665 193.170.140.71 TCP 8645 > http [StN] Seq=0 Ack=1 win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), DSt Port: 54262 (54262) Domain Name System (response) Imaser Rs: 1	17 2.436639	140.78.100.211	65.52.107.149	TCP	8645 > http [AC VVIIALS THIS? INVESTIGATE!
20 2.609521 140.78.100.211 140.78.100.119 DNS Standard query 21 2.791622 Intel_40:e1:0d Broadcast ARP who has 140.78. 22 2.791711 Intel_40:e1:0d Broadcast ARP who has 140.78. 23 2.807614 140.78.100.211 65.52.107.149 TCP B644 > http [A Note: Google Chrome U 24 2.986566 140.78.100.211 140.78.100.211 DNS Standard query AAAA www.bing.com CMME akam.bing.com CNAME al34.]m. akam 25 2.987423 140.78.100.211 193.170.140.71 TCP 8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 ws=8 28 2.993681 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 ws=8 29 2.996685 193.170.140.71 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 ws=8 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 ws=8 193 170.140.71 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 ws=8 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq.4	18 2.437177				
21 2.791682 Intel_40:e1:0d Broadcast ARP who has 140.78. Note: Google Chrome u 22 2.791711 Intel_40:e1:0d Broadcast ARP who has 140.78. Note: Google Chrome u 23 2.807614 140.78.100.211 65.52.107.149 TCP 8644 > http Iad Note: Google Chrome u 24 2.986566 140.78.100.119 140.78.100.119 Ns Standard query response CNAME akam.bing.com CNAME al34.1m.akam 25 2.987423 140.78.100.211 140.78.100.119 Ns Standard query response CNAME akam.bing.com CNAME al34.1m.akam 27 2.993391 140.78.100.211 193.170.140.71 TCP 8648 > http [SNN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 28 2.993682 140.78.100.211 193.170.140.71 TCP 8648 > http [SNN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 20 2.996643 193.170.140.71 140.78.100.211 193.170.140.71 TCP 8648 > http [AxK] Seq=0 Ack=1 win=65192 23 2.996645 193.170.140.71 140.78.100.211 193.170.140.71 TCP 8648 > http [AxK] Seq=0 Ack=1 win=65336 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) Image: Standard Guery response (Standard Guery response, No error) <td< td=""><th>19 2.603541</th><td></td><td></td><td></td><td>HTTP/1.1 301 Md</td></td<>	19 2.603541				HTTP/1.1 301 Md
23 2,807614 140.78.100.211 65.52.107.149 TCP 8644 > http [Ad					Who has 140.78 Notor Cooolo Chromo uc
23 2.807614 140.78.100.211 65.52.107.149 TCP 8644 > http [Ad. 24 2.986566 140.78.100.119 140.78.100.211 DNS Standard query esponse CNAME akam.bing.com CNAME al34.1m.akam 25 2.987423 140.78.100.211 140.78.100.119 DNS standard query AAAA www.bing.com 26 2.992487 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 27 2.993682 140.78.100.211 193.170.140.71 TCP 8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996685 193.170.140.71 140.78.100.211 TCP http> 8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996685 193.170.140.71 140.78.100.211 TCP http> 8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996685 193.170.140.71 140.78.100.211 TCP http> 8648 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 30 2.996742 140.78.100.211 193.170.140.71 TCP 8649 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=8 193.170.140.71 140.78.100.211 TCP http> 8648 [SYN] ACK] seq=0 Ack=1 win=14600 Len=0 MSS=1460 WS 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [ACK] seq=1 Ack=1 win=65336 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Trime: 0.284203000 seconds] Transaction ID: 0x005f ⊞ Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 ⊒ Queries ■ Answers ■ MNwers ■ Maxe: www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) Class: IN (0x0001)					who has 140.78 INOLE. GOOGIE CHIOME US
24 2.986566 140.78.100.119 140.78.100.211 DNS standard query response CNAME akam.bing.com CNAME al34.1m.akam 25 2.992487 140.78.100.119 140.78.100.211 DNS standard query response CNAME akam.bing.com 26 2.992487 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 28 2.993681 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 29 2.993682 193.170.140.71 140.78.100.211 TCP 8648 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 29 2.993685 193.170.140.71 140.78.100.211 TCP 8648 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [ACK] Seq=0 ACK=1 Win=14600 Len=0 MSS=1460 WS=8 29 2.996685 193.170.140.71 140.78.100.211 TCP http > 8648 [SYN, ACK] Seq=0 ACK=1 Win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Time: 0.284203000 seconds] Transaction ID: 0x005f Image: 140.78.100.211 Image: 140.78.100.211 Quertions: 1 Answer SN Additional RRs: 0 Image: 140.78.100.211 </td <th></th> <td>140.78.100.211</td> <td></td> <td></td> <td></td>		140.78.100.211			
25 2.987423 140.78.100.211 140.78.100.119 DNS standard query response CNAME atam.bing.com 26 2.992487 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 27 2.993391 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 28 2.993682 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996685 193.170.140.71 140.78.100.211 TCP 8649 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [ACK] Seq=1 ACK=1 win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Fequest In: 8] [Trime: 0.284203000 seconds] Transaction ID: 0x005f # [Ack] Seq=1 Ack=1 win=65536 Len=0 @ Queries					Standard query response CNAME akam.bing.com CNAME a134.lm.akamai
26 2.992487 140.78.100.119 140.78.100.211 DNS Standard query response CNAME akam.bing.com CNAM	25 2.987423	140.78.100.211	140.78.100.119	DNS	Standard query AAAA www.bing.com
28 2.993682 140.78.100.211 193.170.140.71 TCP 8649 > http [StN] Seq=0 win=8192 Len=0 MSS=1460 WS=8 29 2.996682 193.170.140.71 140.78.100.211 TCP http > 8648 [StN, AcK] Seq=0 Ack=1 win=1460 Us=0 MSS=1460 WS 30 2.996742 140.78.100.211 193.170.140.71 TCP http > 8648 [StN, AcK] Seq=0 Ack=1 win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Trime: 0.284203000 seconds] Transaction ID: 0x005f Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional Rs: 0 E Authority Rs: 0 Www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Name: www.bing.at Type: A (Host address) Class: IN (0x0001) Class: IN (0x0001)	26 2.992487	140.78.100.119	140.78.100.211		Standard query response CNAME akam.bing.com CNAME a134.lm.akamai
29 2.996685 193.170.140.71 140.78.100.211 TCP http > 8648 [svw, Ack] seq=0 Ack=1 win=14600 Len=0 MSS=1460 ws 30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [ACK] seq=1 Ack=1 win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Time: 0.284203000 seconds] Transaction ID: 0x005f # Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 # Queries # Answers @ www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) _ Class: IN (0x0001)					
30 2.996742 140.78.100.211 193.170.140.71 TCP 8648 > http [ACK] seq=1 Ack=1 win=65536 Len=0 User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Time: 0.284203000 seconds] Transaction ID: 0x005f Transaction ID: 0x005f B Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 # B Queries # = Answers # ⊡ www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at: type A, class IN, addr 65.52.107.149 Class: IN (0x0001)					6049 > NLTP [SYN] Seq=0 WIN=8192 Len=0 MSS=1460 WS=8
User Datagram Protocol, Src Port: domain (53), Dst Port: 54262 (54262) Domain Name System (response) [Request In: 8] [Time: 0.284203000 seconds] Transaction ID: 0x005f # Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 # Queries = Answers = Answers = Maswers D www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) Class: IN (0x0001)					8648 > http [ACK] Seg=1 Ack=1 Win=14000 Len=0 MSS=1400 WS=2
<pre> Flags: 0x8400 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries Answers Answers Answers Answers Class: IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) Class: IN (0x0001)</pre>	Domain Name System (res [Request In: 8]	ponse)	Port: 54262 (54262)		
Authority RRs: 0 Additional RRs: 0	⊞ Flags: 0x8400 (Standa)		
Queries Answers Answers www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) Class: IN (0x0001)	Authority RRs: 0				
⊡ www.bing.at: type A, class IN, addr 65.52.107.149 Name: www.bing.at Type: A (Host address) Class: IN (0x0001)					
Name: www.bing.at Type: A (Host address) Class: IN (0x0001)					
Class: IN (0x0001)			149		
		iress)			
	Type: A (Host add				
Data length: 4	Type: A (Host add Class: IN (0x0001	.)			
Addr : 65.52.107.149	Type: A (Host add Class: IN (0x0001 Time to live: 1 h	.)			

Wireshark **HTTP - Request**

Intel(R) PRO/100 VE Network Conn				
	ze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp			211 171 180 Jo 120
		₮ ⊻ ■ 🖬 Ѳ, Ѳ		
Filter:		Expression Clear Apply		
No Time	Source	Destination	Protocol	Info
11 2.315500 12 2.316318	140.78.100.119 140.78.100.211	140.78.100.211 65.52.107.149	DNS TCP	Standard query response 8644 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
13 2.316646	140.78.100.211	65.52.107.149	ТСР	8645 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
14 2.436395	65.52.107.149	140.78.100.211	TCP	http > 8644 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 WS=0
15 2.436499	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
16 2.436609 17 2.436639	65.52.107.149 140.78.100.211	140.78.100.211 65.52.107.149	TCP TCP	http > 8645 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 WS=0 8645 > http [ACK] Seq=1 Ack=1 win=65536 Len=0
18 2.437177	140.78.100.211	65.52.107.149	НТТР	GET / HTTP/1.1
19 2.603541	140.78.100.211 65.52.107.149	140.78.100.211	HTTP	HTTP/1.1 301 Moved Permanently
20 2.609521 21 2.791682	140.78.100.211 Intel 40:e1:0d	140.78.100.119 Broadcast	DNS ARP	Standard query A www.bing.com who has 140.78.100.141? Tell
22 2.791711	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell What are these? In
Hypertext Transfer Proto	col			
Request URI: / Request Version: HTT	P/1.1			
Host: www.bing.at\r\n				
Connection: keep-alive User-Agent: Mozilla/5.	0 (Windows NT 6.1; WOW64)			Secko) Chrome/18.0.1025.168 safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/5. Accept: text/html,appl	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat			Secko) Chrome/18.0.1025.168
Connection: keep-alive User-Agent: Mozilla/5. Accept: text/html,appl Accept-Encoding: gzip,	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat	ion/xml;q=0.9,*/*;q=0.		Secko) Chrome/18.0.1025.168
Connection: keep-alive User-Agent: Mozilla/5. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE	0 (windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n	ion/xml;q=0.9,*/*;q=0. =0.4\r\n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/5. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE	0 (windows NT 6.1; WOW64) / ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-U5;q=0.6,en;q	ion/xml;q=0.9,*/*;q=0. =0.4\r\n		5ecko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive USer-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		5ecko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		5ecko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		secko) Chrome/18.0.1025.168 safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xm1;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Encoding: gzip, Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (Windows NT 6.1; WOW64) ication/xhtml+xml,applicat deflate,sdch\r\n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r	ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n
Connection: keep-alive User-Agent: Mozilla/S. Accept: text/html,appl Accept-Language: de-DE Accept-Charset: ISO-88 \r\n	0 (windows NT 6.1; wow64) ication/xhtml+xml,applicat deflate,sdchr/n ,de;q=0.8,en-US;q=0.6,en;q 59-1,utf-8;q=0.7,*;q=0.3\r 06 2f e9 8c 4e 64 d3 41 3 fd f0 00 b8 d9 50 cc 50 1 45 54 20 2f 20 48 54 54 5 56 73 74 3a 20 77 77 72 60 0a 43 6f 6e 69 76 65 0 67 65 6e 74 3a 20 4d 6f 7 31 3b 20 57 4f 57 36 34 2 56 62 4f 66 46 4f 7 31 3b 20 57 4f 57 36 34 2 56 62 4f 66 62 6f 65 2f 56 2e 31 39 00 a 41 63 6f 6 20 43 68 72 6f 66 65 2f 57 65 6e 74 66 74 65 6f 6 20 43 68 72 6f 66 65 2f 53 2e 31 36 38 20 53 61 6 26 39 26 63 174 69 6f 6e 2 27 4 2f 68 74 64 66 2c 61 7 28 39 2c 2a 2f 2a 3b 71 3 53 66 174 69 6f 6e 2 29 39 2c 2a 2f 2a 3b 71 3 53 65 70 74 2d 55 66 36 2f 38 2c 65 6e 2d 55 53 3b 7 38 71 30 2e 34 04 0a 4 61 72 73 65 74 3a 20 4 43 30 2e 33 04 0a 04 51 72 73 65 74 3a 20 4 51 74 2f 66 2d 55 55 3b 7 38 71 30 2e 34 04 0a 4 51 72 73 65 74 3a 20 4 51 73 65 74 3a 20 4 51 74 26 2d 38 2 39 71 30 2e 33 04 0a 7 20 31 2c 75 74 66 2d 38 2 39 71 30 2e 33 04 0a 7 30 71 30 72 36 7 30 71 30 72 36 7 30 71 30 7 30 71 30 7 30 71 30 7 30 71 30 7 30	<pre>ion/xml;q=0.9,*/*;q=0. =0.4\r\n \n 34+q@ /Nd.A4 86 k.!.PP.P. 70GE T / HTTP 70GE T / HTTP 71 11A/5.0 (Window 74 bing.atConnect 16 ion: kee p-alive. 71 illa/5.0 (Window 72 illa/5.0 (Window 72 illa/5.0 (Window 72 illa/5.0 (Window 73 NT 6.1; WWW64) 16 Gecko) Chrome! 17 Ml,application/xhtml+ 17 xml,application/xhtml+ 17 xml;q=0.9,*/*;q= 16 0.8Acc ept-Enco 16 ding;gz ip,defla 17 cal,applicationeccept- 18 deig=0.8,en-US;q 19 e0.6,en; q=0.4.A 19 ccept-ch arset: I 18 b0-8859=1,utf-8; 19 q=0.7,*; q=0.3 19 ccept-0.3 10 ccept-0.3 11 ccept-0.3 11 ccept-0.3 12 ccept-0.3 13 ccept-0.3 14 ccept-0.3 15 ccept-</pre>		Secko) Chrome/18.0.1025.168 Safari/535.19\r\n

Wireshark HTTP - Response

File Edit View Co. Conture An	nnection - Wireshark alyze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp			
	💥 🔁 📇 🔍 🗢 🛸 🎝 🧏		(1) 🕅 👔	
Filter:		Expression Clear Apply		
. ,	Source			Info
No Time 13 2.316646	140.78.100.211	Destination 65.52.107.149	Protocol	8645 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
14 2.436395	65.52.107.149	140.78.100.211	TCP	http > 8644 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=0
15 2.436499	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
16 2.436609 17 2.436639	65.52.107.149 140.78.100.211	140.78.100.211 65.52.107.149	TCP TCP	http > 8645 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS= 8645 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
18 2.437177	140.78.100.211	65.52.107.149	НТТР	GET / HTTP/1.1
19 2.603541	65.52.107.149	140.78.100.211	HTTP	HTTP/1.1 301 Moved Permanently
20 2.609521	140.78.100.211	140.78.100.119	DNS	Standard query A www.bing.com
21 2.791682 22 2.791711	Intel_40:e1:0d Intel_40:e1:0d	Broadcast Broadcast	ARP ARP	who has 140.78.100.141? Tell 140.78.100.129 who has 140.78.100.138? Tell 140.78.100.129
23 2.807614	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] Seq=396 Ack=302 Win=65280 Len=0
24 2.986566	140.78.100.119	140.78.100.211	DNS	Standard query response CNAME akam.bing.com CNAME a134.lm.akam
	NAV STA LOC CURa DEVa PSAa P ATS=1337341091; domain=.bing.			
<pre>□ Content-Length: 0\r\r [Content length: 0] \r\n</pre>	1			
0010 01 55 8c 51 40 00 e 0020 64 d3 00 50 21 c4 b	8 d9 50 cc b7 fd f1 8b 50 18 8 54 54 50 2f 31 2e 31 20 33 5 64 20 50 65 72 6d 61 6e 63	dP! PP. 3]HT TP/1.1 3 5 01 Moved Permane		
0030 12 a7 88 5d 00 00 4 0040 30 31 20 4d 6f 76 6 0050 6e 74 6c 79 0d a 4 0060 72 6f 6c 3a 20 6e 6 0070 6f 63 61 74 69 6f 6	f 2d 63 61 63 68 65 0d 0a 4/	rol: no- cacheL		

Michael Sonntag

P3P Compact Policy: http://www.p3pwriter.com/LRN_111.asp

Wireshark HTTP - Stream

Collow TCP Stream	-	
Stream Content		
GET /?cc=at HTTP/1.1		
Host: www.bing.com		4
connection: keep-alive		
User-Agent: Mozilla/5.0 (windows NT 6.1; WOW64) ApplewebKit/535.19 (KHTML,	like Gecko) Chrome/18.0.1025.168	
Safar 1/535.19		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8		
Accept-Encoding: gzip,deflate,sdch		
Accept-Language: de-DE, de; q=0.8, en-US; q=0.6, en; q=0.4		
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3		
НТТР/1.1 200 ОК		
Cache-Control: private, max-age=0		
Content-Type: text/html; charset=utf-8		
P3P: CP="NON UNI COM NAV STA LOC CURA DEVA PSAA PSDA OUR IND"		
Vary: Accept-Encoding		
Content-Encoding: gzip		
Date: Fri, 18 May 2012 11:38:11 GMT		
Content-Length: 10051		
Connection: keep-alive		
Set-Cookie: _FS=mkt=de-AT&NU=1; domain=.bing.com; path=/		
<pre>Set-Cookie: _SS=SID=9C9E9DA7CB2B43F8B5832A8854ECF181; domain=.bing.com; pa</pre>	th=/	
set-Cookie: MUID=264FA59BF1D561753F42A6FFF0D26193; expires=Sun, 18-May-201		
path=/	· 11/50/11 and, domain forngroom,	
Set-Cookie: OrigMUID=264FA59BF1D561753F42A6FFF0D26193%2c5546792e35a8415997	835740de96da67: expires=5un. 18-	
May-2014 11:38:11 GMT; domain=.bing.com; path=/	obbi foucooutor, expires buil, 10	
set-cookie: srcHD=D=2303258&MS=2303258&AF=NOFORM; expires=sun, 18-May-2014	11:38:11 GMT: domain=.bing.com: path=	:/
<pre>Set-Cookie: SRCHUID=V=2&GUID=EFF4F73D88574A12B17D3F6371AEC69D; expires=Sun</pre>		'
<pre>Set-Cookie: SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20120518; expires=Sun, 18-May=</pre>	2014 11:38:11 GMT; domain=.bing.com;	
path=/	· · · · · ·	
	@5.2@ "@^v	•
\Bffb/b/oId9h6wj.a4k.o~AX&6Dj hbw.OHh.x\$&~.v4d.8"5".z#y\BoeR.w`.Rr.l=.y~.	.KN.Y, RR@7>/	
hbw.OHh.X\$&~.V4d.8"S".z#y∖BoeR.w`.Rr.l=.y~.,	/.7fk.!8lnMA.	•
Find Save As Print Entire conversation (113759 bytes)	▼ O ASCII O EBCDIC O Hex Dump O C Arrays ●	Ra
Help	Filter Out This Stream Close	

E

Wireshark HTTP - Stream

- Keep-alive: Requested by browser and accepted by sender
 - → Result: After the end of the first response, there follows immedaitely the next request and response
- Content-Encoding: gzip
 - → The content would have to be saved as a binary file and then unzipped to access it (selecting & copying won't work!)
- Response: Normal response headers, P3P information and lots of cookies!
 - → 7 cookies, but note: we didn't send even a single one!
 » Would have been in the request header
 - → Careful: Second request in this stream already knows the headers and does send them with the request!

Wireshark HTTP - Stream

C Follow TCP Stream	_ 🗆 ×
-Stream Content	
\$m6.@kPH.B <x.:`.gt'akt;1< td=""><td></td></x.:`.gt'akt;1<>	
gC=#Tz Ve7[r.5H7#'3:.FX .d <gw.)(@ui.?`\$s~.g4vo< td=""><td></td></gw.)(@ui.?`\$s~.g4vo<>	
H.1.qm2=.{.21h{E2f6sM`.t.Wm.%.D^{.p9.U	
[3~.to'eguy.}fq.]bs.) GDc^MH.?=.01.g}d~	
\$Bl2.7@.9.g.[z2f.SAsC0r\x./.4.UK.Y2	
' za.`y.gs\$0.IH.IH5.V.00`.(.k.!.M.d).,".m (t.Edo#`*.x.1m6C?8".i.*.8.P/MK.*.'/8.y]i&L.	
(t.Edo#`*.x.1m6C?8"i*8.P/MK.*.'/8.y1i&L.	
%;.M{^[B. V.:m%%L1.92)eg9.b5.Pfv".%p.5.r.KY*OMN#.Pk7shiE.g.)	
n./.e.>~=4.#0.YMAG.4xj.FMSjkxiri.fY`.P[FtJ+Gj/"/	
. (CQ^#.#	
HTTP/1.1	
Host: www.bing.com	
Connection: keep-alive	
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168	
Safari/535.19	
Accept: */*	
Referer: http://www.bing.com/?cc=at	
Accept-Encoding: gzip,deflate,sdch	
Accept-Language: de-DE, de; q=0.8, en-US; q=0.6, en; q=0.4	
Accept-Charset: ISO-8859-1, utf-8; q=0.7, *; q=0.3	
Cookie: _FS=mkt=de-AT&NU=1; _SS=SID=9C9E9DA7CB2B43F8B5832A8854ECF181; MUID=264FA59BF1D561753F42A6FFF0D26193;	
OrigMUID=264FA59BF1D561753F42A6FFF0D26193%2c5546792e35a8415997835740de96da67;	
SRCHD=D=2303258&MS=2303258&AF=NOFORM; SRCHUID=V=2&GUID=EFF4F73D88574A12B17D3F6371AEC69D; SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20120518	
SKCHUSK=AUTOKEDIK=U@GEUVAK=@DUB=20120318	
НТТР/1.1 200 ОК	
Content-Length: 8901	
Content-Type: image/png	
Last-Modified: Mon, 10 Oct 2011 18:35:52 GMT	
X-N: 5	
Cache-Control: public, max-age=12463992	
Date: Fri, 18 May 2012 11:38:12 GMT	_
pater int, to may fore insome and	
Eind Save As Print Entire conversation (113759 bytes) Find Save As Print Entire conversation (113759 bytes) O ASCII C BECDIC O Hex Dump O C Arrays	Raw
Help Filter Out This Stream Close	
Help Filter Out This Stream Close	

E

Wireshark HTTP authentication

Intel(R) PRO/100 VE Network Con	nection - Wireshark			
	lyze <u>Statistics</u> Telephon <u>y</u> <u>T</u> ools <u>H</u> elp			
	※ ₴ 븝 수 수 🎝	77 ⊉ 🗏 📑 €, €	ζ 🔍 🖭	🛎 🗹 幆 🔆 🛱
Filter: http		 Expression Clear Apply 		
No. Time	Source	Destination	Protocol	Info -
13 6.804169	140.78.100.211	213.165.65.100	HTTP	POST /de/cgi/login HTTP/1.1 (application/x-www-form-urlencoded)
15 6.945697 19 6.985769	213.165.65.100 140.78.100.211	140.78.100.211 213.165.64.71	НТТР НТТР	HTTP/1.1 302 Found (text/html) GET /?status=login-failed HTTP/1.1
21 7.019225	213.165.64.71	140.78.100.211	НТР	HTTP/1.1 301 Moved Permanently (text/html)
25 7.058273	140.78.100.211	213.165.64.72	НТТР	GET /?status=login-failed HTTP/1.1
42 7.180847	213.165.64.72	140.78.100.211	HTTP	HTTP/1.1 200 OK (text/html)
47 7.568014	140.78.100.211	213.165.64.72	HTTP	GET /uim.html HTTP/1.1
50 7.597259 51 7.607270	140.78.100.211 213.165.64.72	217.72.204.172 140.78.100.211	HTTP HTTP	GET /ngvar.js HTTP/1.1 HTTP/1.1 200 OK (text/html)
52 7.623443	140.78.100.211	2.21.93.234	HTTP	Continuation or non-HTTP traffic
55 7.630422	217.72.204.172	140.78.100.211	НТТР	HTTP/1.1 200 OK (application/x-javascript)
64 7.831915	140.78.100.211	217.72.203.250	нттр	GET /?LogoutAdProxy.service=hpfirst&site=gmx§ion=gmx/homepage
 Transmission Control Pr Hypertext Transfer Prot POST /de/cgi/login HT ⊕ [Expert Info (Chat/ Request Method: POS Request URI: /de/cg 	otocol, Src Port: 12107 (12 ocol TP/1.1\r\n Sequence): POST /de/cgi/log T i/login			
Transmission Control Pr → Hypertext Transfer Prot → POST /de/cgi/login HT → [Expert Info (Chat/ Request Method: POS Request Version: HT Host: service.gmx.net Connection: keep-aliv → [Content length: 116\r [Content length: 116\r [Content length: 11 Cache-Control: max-ag Origin: http://www.gm User-Agent: Mozilla/5 Content-Type: applica Accept: text/html,app Referer: http://www.g Accept-Encoding: gzip Accept-Language: de-D Accept-Charset: ISO-8	otocol, Src Port: 12107 (12 ocol TP/1.1\r\n Sequence): POST /de/cgi/log T i/login TP/1.1 \r\n e\r\n e\r\n \n 6] e=0\r\n x.at\r\n .0 (Windows NT 6.1; WOW64) tion/x-www-form-urlencoded tication/xhtml+xml,applicat mx.at/?status=login-failed	107), Dst Port: http (in HTTP/1.1\r\n] ApplewebKit/535.19 (КН r\n ion/xml;q=0.9,*/*;q=0. r\n =0.4\r\n	80), Seq: 1 TML, like d	
Transmission Control Pr → Hypertext Transfer Prot → POST /de/cgi/login HT → [Expert Info (Chat/ Request Method: POS Request Version: HT Host: service.gmx.net Connection: keep-aliv → Content-Length: 116\r [Content length: 11 Cache-Control: max-ag origin: http://www.gm User-Agent: Mozilla/5 Content-Type: applica Accept: text/html,app Referer: http://www.g Accept-Encoding: gzip Accept-Charset: ISO-8 \r\n → Line-based text data: a	otocol, Src Port: 12107 (12 ocol TP/1.1\r\n Sequence): POST /de/cgi/log T T/1.1 \r\n e\r\n \n 6] e=0\r\n x.at\r\n .0 (Windows NT 6.1; WOW64) tion/x-www-form-urlencoded\ lication/xhtml+xml,applicat mx.at/?status=login-failed\ ,deflate,sdch\r\n E,de;q=0.8,en=US;q=0.6,en;q &S9=1,utf=8;q=0.7,*;q=0.3\r pplication/x-www-form-urlen xr2=&dleve1=c&id=test%40gmx	<pre>107), Dst Port: http (in HTTP/1.1\r\n] ApplewebKit/535.19 (KH r\n ion/xm];q=0.9,*/*;q=0. r\n =0.4\r\n \n coded .at&p=password&jsenabl g pt=(nars et: 150-</pre>	80), Seq: 1 TML, like C 8\r\n	, Ack: 1, Len: 700

Wireshark

HTTP authentication + TLS

Intel(R) PRO/100 VE Network Conn				
	yze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp			
	🗙 🔁 占 🔍 🍬 🔶 🤪	77 ⊈ 🗏 📑 €, €	l 🔍 🖭 i	
Filter: ssl http		Expression Clear Apply		
No Time	Source	Destination	Protocol	Info
20 1.708613	140.78.100.211	213.165.65.100	TLSV1	Client Hello
22 1.765842 24 1.765849	213.165.65.100 213.165.65.100	140.78.100.211 140.78.100.211	TLSV1 TLSV1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
26 1.792478	140.78.100.211	213.165.65.100	TLSV1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message,
27 1.834206	213.165.65.100	140.78.100.211	TLSV1	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake M
28 1.892803	213.165.65.100	140.78.100.211	TLSV1	Application Data, Application Data
37 1.983291 39 2.016840	140.78.100.211 213.165.64.71	213.165.64.71 140.78.100.211	НТТР НТТР	GET /?status=login-failed HTTP/1.1 HTTP/1.1 301 Moved Permanently (text/html)
47 2.118085	140.78.100.211	213.165.64.72	НТТР	GET /?status=login-failed HTTP/1.1
62 2.242440	213.165.64.72	140.78.100.211	HTTP	HTTP/1.1 200 OK (text/html)
67 2.591299 70 2.618334	140.78.100.211 140.78.100.211	213.165.64.72	НТТР	GET /uim.html HTTP/1.1 GET /ngvar.is HTTP/1.1
Version: TLS 1.0 (0x	x0301)			
Length: 3256 ☐ Handshake Protocol: Handshake Type: Ce Length: 3252 Certificates Lengt ☐ Certificates (3249 Certificate Leng ⑧ Certificate Leng Certificate Leng	Certificate ertificate (11) th: 3249 9 bytes) gth: 1007 -at-commonName=service.gmx. gth: 1136			
Length: 3256 Handshake Protocol: Handshake Type: Ce Length: 3252 Certificates Lengt Certificates (3249 Certificate Leng Certificate Leng	Certificate ertificate (11) th: 3249 9 bytes) th: 1007 -at-commonName=service.gmx. th: 1136 -at-commonName=Thawte SSL C th: 1097 -at-commonName=thawte Prima andshake Protocol: Server K nake (22)	A,id-at-organizationNa ry Root CA,id-at-organ	me=Thawte,	5MX,id-at-organizationName=1&1 Mail & Media GmbH,id-at-localityName=Mont Inc.,id-at-countryName=US) itName=(c) 2006 thawte, Inc For author,id-at-organizationalUnitName=C
Length: 3256 Handshake Protocol: Handshake Type: Ce Length: 3252 Certificates Lengt Certificates (3249 Certificate (id- Certificate Leng Certificate Leng Certificate (id- Certificate Leng Certificate Leng Certificate Leng TLSv1 Record Layer: Ha	Certificate ertificate (11) th: 3249 9 bytes) gth: 1007 -at-commonName=service.gmx. gth: 1136 -at-commonName=Thawte SSL C gth: 1097 -at-commonName=thawte Prima andshake Protocol: Server K nake (22) k0301)	A,id-at-organizationNa ry Root CA,id-at-organ	me=Thawte,	Inc.,id-at-countryName=US)
Length: 3256 Handshake Protocol: Handshake Type: Ce Length: 3252 Certificates Lengt Certificates (3249 Certificate Leng Certificate (id- Certificate Length: 525	Certificate ertificate (11) th: 3249 9 bytes) gth: 1007 -at-commonName=service.gmx. gth: 1136 -at-commonName=Thawte SSL C gth: 1097 -at-commonName=thawte Prima andshake Protocol: Server K nake (22) k0301) Server Key Exchange	A,id-at-organizationNa ry Root CA,id-at-organ ey Exchange	me=Thawte, izationalUn	Inc.,id-at-countryName=US)

Serial number: Photograph



Code: NAR61HA06E040L0711214

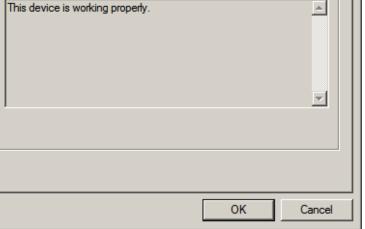
• E1245D7N

Michael Sonntag

F

Serial number: According to tools

Drive Name	Serial Number	Revision	Attached		
E040L0	ABCDEF0000125EF7	NAR6	Yes		
				Maxtor 6 E040L0 USB Device Properties	
				Maxtor 6 E040L0 0SB Device Properties	
				General Policies Volumes Driver Details	
Help-About	New Firmware	Check	Close	Maxtor 6 E040L0 USB Device	
http://suppo	ort.seagate.com/firmw	vare/drive_c	onfia html	Device type: Disk drives	
nup.//suppo	nt.seayate.com/mmw	are/unve_c	onng.num	Manufacturer: (Standard disk drives)	



F[∐]

X

Serial number: X-Ways Forensic

I	Technical Details Report	×	
	K-Ways Forensics 14.1 SR-2 13.10.2011, 08:54:05 Hard disk 7 Model: Maxtor 6E040L0 Serial No.: \$á Firmware Rev.: NAR6 Bus: USB Total capacity: 41.110.142.976 bytes = 38,3 GB		
	Number of cylinders: 4.998 Number of heads: 255 Sectors per track: 63 Bytes per sector: 512 Sector count: 80.293.248 Sector count: ? [according to ATA] Unpartitionable space: 378 Sectors		
	Partition 1 Sectors 63 - 208.844 Partition table: Sector 0 File system: Ext3 Total capacity: 106.896.384 bytes = 102 MB Sector count: 208.782 Bytes per sector: 512 Bytes per cluster: 1.024 Free clusters: 72.627 = 70% free Total clusters: 104.388		
	Close	Help	

7世

F

Serial number: Web information

Maxtor DiamondMax Plus 8



Serial Number Locator



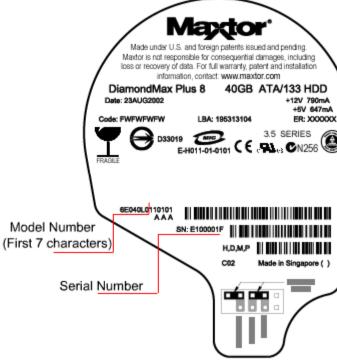
This label type can be found on the following Maxtor drive model:

Diamondmax Plus 8

Main Menu

SeaTools for Windows is a comprehensive, easy-to-use diagnostic tool that helps you quickly determine the condition of the disc drive in your external hard drive, desktop or notebook computer. It includes several tests that will examine the physical media on your Seagate or Maxtor disc drive and any other non-Seagate disc drive. SeaTools for Windows tests USB, 1394, ATA (PATA/IDE), SATA and SCSI drives. It installs onto your system. SeaTools for Windows is completely data safe. Download SeaTools

Print



http://support.seagate.com/kbimg/flash/serial_number_locator/SerialNumberLocator.html

 $(]]^{\downarrow}$

Disk image

- Variant A: SelfImage (or other tools
 - → Useful tool, no forensic support
 - \rightarrow Problem: Finding the correct disk
 - → No timing/estimate
 - → Ca. 500 MB/min
- Variant B: dcfldd
 - Problem: "Permission denied" on Windows 7
- Variant C: X-Ways Forensic
 - → Only complete drives or logical drives (=has a drive letter); no partitions
 - \rightarrow Full version needed (or only 200 kB!)
 - → Must be run as Administrator
- → Ca. 850 MB/min

SelfIm	iage v1	.2 _ 🗆 🗙
ile <u>E</u> dit	<u>H</u> elp	
Status		
		3%
		Input Size 38.287GB
Input:	\Devic	e\Harddisk7 (entire disk)
Output:	C:\Dat	a\tmp\disk.img.gz
Byte	es read:	1.262 GB
S	kipped:	N/A
Bytes	written:	575.511MB
Current	speed:	9.916MB/s
Average	speed:	8.304MB/s
		Start Cancel

Transferring sectors (No. 7110144)	×
9%	
approx. 19 min. left	_

Disk image

- Variant D: OSFClone
 - \rightarrow Self-booting (CD, USB, ...)
 - → Free tool
 - → Formats: Raw, AFF
 - → http://www.osforensics.com/tools/create-disk-images.html
- Variant E: FTK Imager
 - → Free part of the commercial product "FTK"
 - Installable version and portable one available
 - Windows program
 - → Formats: Raw, AFF, Encase
 - → Supports also preview, obtaining copy of protected files (registry), …

Questions?

Thank you for your attention!

F[∐][♠]

Literature/Links

E

- NMap http://nmap.org/
- Wayback Machine http://www.archive.org/web/web.php
- DomainTools Whols http://whois.domaintools.com
- MX Toolbox http://www.mxtoolbox.com/
- Wireshark http://www.wireshark.org/