

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 2012



Agenda

- NMap
- Web caches
- Web Archive
- Whols
- MX-Records
- Wireshark

Michael Sonntag

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!
 - → Services → 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"
 - → Interpret the results
 - » Correct output?
 - » Something surprising/dangerous found?

Sample result: NMap local subnet scan

	-M	Sample result
\square	$\Pi \leq \square$	NMan local subnet sca
IF		
	👁 Zenmap	
	Sc <u>a</u> n Werk <u>z</u> euge <u>P</u> rofil <u>H</u> ilfe	
	Ziel: 140.78.100.128/25	Profil: Ping scan Scan Abbrechen
	Befehl: nmap -sn 140.78.100.128/	25
	Rechner Dienste	Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans
	Retriehssystem	nmap -sn 140.78.100.128/25 🗾 Details
	r1-intern.fim.un	MAC Address: 00:11:85:C9:62:A0 (Hewlett Packard)
	hp2824-1a.fim.u	Host is up (0.0020s latency).
	mpic3f08e.fim.u	<u>MAC Address:</u> 00:30:C1:C3:F0:8E (Hewlett-packard) Nmap scan report for hplim602.fim.uni-linz.ac.at (140.78.100.140)
	hpljm602.fim.ur	Host is up (0.00s latency).
	praher-vista32.	Nmap scan report for praher-vista32.fim.uni-linz.ac.at (140.78.100.162)
	inge_xp.ads2-fi	Host is up (0.00s latency). MAC Address: 00:10:00:18:44:58 (Intel Corporate)
	140.78.100.168	Nmap scan report for inge_xp.ads2-fim.fim.uni-linz.ac.at (140.78.100.165)
	sabine-win7.ads	Host is up (0.0010s latency). MAC Address: 00:1C:C0:32:C9:3C (Intel Corporate)
	140.78.100.206	Nmap scan report for 140.78.100.168
	140.78.100.208	MAC Address: 00:18:FE:D0:EA:40 (Hewlett Packard)
	michael_w7.ads	Nmap scan report for sabine-win7.ads2-fim.fim.uni-linz.ac.at (140.78.100.205) Host is up (0.00s latency).
	jrm_win7.ads2-	MAC Address: E0:69:95:4F:F7:03 (Unknown)
	140.78.100.250	Nmap scan report for 140.78.100.206 Host is up (0.00s latency).
	140.78.100.251	MAC Address: 00:22:15:A9:DD:A1 (Asustek Computer)
		Host is up (0.00s latency).
		MAC Address: 40:60:8F:46:EB:48 (Unknown) Nman scan report for michael w7.ads2-fim.fim.upi-lipz.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)
		Host is up (0.0030s latency).
		MAC Address: 00:04:23:D3:FB:5C (Intel)
		Host is up (0.00s latency).
		MAC Address: 00:04:23:D3:FB:5A (Intel) Nmap done: 128 IP addresses (14 hosts up) scanned in 2.73 seconds
	Filtere Rechner	

FU -	
Rechnerbetrachter	
Hosts Allgemein Dienste Traceroute	
r 1-inte router Allgemeine Informationen	
inge_s Adresse: [ipv4] 140.78.100.31	-
habib.t jrm_w: Rechnername: [PTR] router.fm.uni-linz.ac.at hplj41(•
hp282- 🕒 Betriebssystem	
hp282- Benutzte Ports: 1/tcp dosed	•
alex_v praher Fingerabdruck Fingerabdruck	
cs140- % • Vendor • Type • Family • Version	•
140.7E 100 Cisco router IOS 12.X	
fim_ma hoer_>	
npi805 Reihen	rachter

1	⋗ Recl	ine	rbe	tra	chter					<u> </u>
	Hosts	4	A	lgerr	nein Dien	ste Tracero	ute			
	r 1-inte			Dort	(E)			land 1		
	router.			FUL		raports (995)) [Speziairei	lder		
	inge_s			Po	rt 🔳	Protocol 4	State 🔹	Service 4	Method	
	habib.t				135	tcp	filtered	msrpc	table	
	jrm_w:			L	135	state	reason_ip			
	hplj41(L	135	state	state	filtered		
	hp282			L	135	state	reason			
	hp282			L	135	state	reason_ttl			
	hp262			L	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	
	-1-1-1-			I.	502	ten	filtered	http://penman	tahla	
				_						

	5/	M		Sample resu
Í	同世的			NMap ir
ļ		👁 Zenmap		
		Sc <u>a</u> n Werk <u>z</u> euge <u>P</u> rofil <u>H</u>	ilfe	
		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.fim.uni-linz.ac.at (140.78.100.31) Kommentare	
		router.fi		
		₩ hp2626-	Status: up	
		🕨 hp2824-	Geöffnete Ports: 0	
		₩ hp2824-	Getilterte Ports: 5 Geschlossene Ports: 995	
		M hplj4100	Gescannte Ports: 1000	
		🥶 npi8054	Laufzeit: Not available	
		yrm_w/.a	Letzter Systemstart: Not available	
		alex v6	Adressen	
		w hoer_xp	IPv4: 140.78.100.31	
		Je alex_w2	MAC: Not available	
		💹 cs140-78		
		🐓 fim_mad	Name - Typ: router fm uni-linz ac at - PTR	
		💯 praher-v	Nume Typ: Todel time in 2 delate The	
		💹 son_vist		
		J40.78.		
		💹 inge_sta		
		Filtere Rechner		

	m /A	1/	Sample res	
F	<u>U</u> S		NMap i	
	👁 Zenmar)		
	Sc <u>a</u> n Wer	rk <u>z</u> euge <u>P</u> rofil	Hilfe	
	Ziel: 140.	.78.100.31	Profil: Comprehensive Scan Abbrechen	
	Befehlt or	Te Ver Sector		
	berenit. Jui			
	Rechner	Dienste	Nmap-Ausgabe Ports / Rechner Netzstruktur Rechner-Details Scans	
	Betriebssyst	tem (Rechner	nmap -sS -sU -sV -T4 -O -A -v -PE -PM -PP -PS -PA -PU -PO -PY 140.78.100.31	
		router.fi	Discovered open port 161/udp on 140.78.100.31	
		r 1-intern	Initiating Service scan at 15:21	
		hp2626-	Scanning 5 services on router.fim.uni-linz.ac.at (140.78.100.31)	
		bp2824-	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)	
		hp2021	Initiating OS detection (try #1) against router.fim.uni-linz.ac.at (140.78.100.31)	
		hp202+	Initiating Traceroute at 15:22	
		npij4100	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.a	NSE: Script scanning 140.78.100.31.	
	Sec. 19	habib.fin	Completed NSE at 15:23, 5.01s elapsed	
		alex_v64	Nmap scan report for router.fim.uni-linz.ac.at (140.78.100.31)	
		hoer_xp	Not shown: 1984 closed ports	
1		alex_w2	PORT STATE SERVICE VERSION	
		cs140-7	135/tcp filtered msrpc	
6		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:	
		lige_sta	system: cisco	
			I leap: 0	

	M	Sample re	SU
FU'		NMap	in
	 praher-v son_vist 140.78.: inge_sta 	<pre>1434/top filtered ms-sql-m 67/udp open intp 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 reftime: 0xD17CF541.55BF39S i poll: 6 i clock: 0xD17CF541.55BF39S i profilered msrpc i structure i structure i</pre>	
	Filtere Rechner	OS and Service detection performed. Please report any incorrect results at http://nmap.org/ submit/ . <u>Nmap done:</u> 1 IP address (1 host up) scanned in 909.68 seconds Raw packets sent: 2296 (84.307KB) Rcvd: 2040 (98.464KB)	▼

Google Cache

- The cache gives you access to old/removed content
 - → 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
 - \rightarrow Add "&strip=1" to the search URL
- Not necessarily complete: Some elements or pages might not be cached (recently/at all)
 - Also: Only the last version is available!

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?
 - \rightarrow 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, ...
 - → 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)
 - → You would have to regularly store a copy
- Owner: "Johannes Kepler Universitaet"
- www.jku.at
 - \rightarrow Might have a different IP from inside the university and outside
 - → Outside: Proxies might be involved (not necessarily visible!)

DNS/WhoIs – 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/WhoIs – 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.uni- .ac.at	-linz
fim.uni-linz.ac.at MX preference = 5, mail exchanger = smtp.fim.uni-lin	nz.ac
fim.uni-linz.ac.at MX preference = 10, mail exchanger = maill.edvz.uni-	-linz
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 >	

FUM

DNS/Whols – MX records

$\sim M$				
11/5			D	NS/Whols – MX
🔮 root@mail:~				
[root@mail ~]# o	dig -t MX fim.u	ni-lin	z.ac.at	-
; <<>> DiG 9.7.4 ;; global option ;; Got answer: ;; ->>HEADER<<- ;; flags: gr rd	4-RedHat-9.7.4-3 ns: +cmd opcode: QUERY, ra; OUERY: 1, 2	1.el5 - statu: ANSWER	<<>> -t MX s: NOERROR, : 2, AUTHOR	fim.uni-linz.ac.at , id: 9067 RITY: 4, ADDITIONAL: 8
				·
;; QUESTION SECT	FION:			
;fim.uni-linz.ad	c.at.	IN	MX	
;; ANSWER SECTION	ON:			
fim.uni-linz.ac	.at. 5532	IN	MX	20 mail2.edvz.uni-linz.ac.at.
fim.uni-linz.ac	.at. 5532	IN	MX	10 maill.edvz.uni-linz.ac.at.
· · AUTHORITY SEC	TTON.			
fim.uni-linz.ac	.at. 5532	TN	NS	aliiku01.edvz.uni-linz.ac.at.
fim.uni-linz.ac	.at. 5532	IN	NS	ns1.fim.uni-linz.ac.at.
fim.uni-linz.ac	.at. 5532	IN	NS	ns2.jku.at.
fim.uni-linz.ac	.at. 5532	IN	NS	ns2.fim.uni-linz.ac.at.
;; ADDITIONAL SE	ECTION:			
mail1.edvz.uni-1	linz.ac.at. 194	6 IN	A	140.78.3.68
mail1.edvz.uni-1	linz.ac.at. 194	6 IN	AAAA	2001:628:2010:2::68
mail2.edvz.uni-1	linz.ac.at. 1933	2 IN	A	140.78.3.69
mail2.edvz.uni-1	linz.ac.at. 1933	2 IN	AAAA	2001:628:2010:2::69
ns1.fim.uni-lin:	z.ac.at. 7177	IN	A	140.78.100.48
ns2.fim.uni-lin:	z.ac.at. 7177	IN	A	140.78.100.49
ns2.jku.at.	46599	IN	A	140.78.3.62
alijku01.edvz.um	ni-linz.ac.at.	1932 II	A N	140.78.2.62
;; Query time: 2	2 msec			
;; SERVER: 127.0	0.0.1 # 53 (127.0.0	0.1)		
;; WHEN: MON OCT	c IU II:I9:II 20	011		

Michael Sonntag

F

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

- 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 → Modification of behaviour
 - » Binaries (or even the network driver) might be modified
 - → 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 $\ensuremath{\textcircled{}{\odot}}$
- Software for this:
 - \rightarrow 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

Michael Sonntag

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 N	etwork Connection: \Device\WPF_{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 megabyte(s)
Limit each packet to 1 bytes	
Capture Filter:	•
Capture File(s)	Display Options
File: Browse	· Update list of packets in real time
Use <u>m</u> ultiple files	
Next file every 1 megabyte(s)	▲utomatic scrolling in live capture
Next file every 1 minute(s)	Hide capture info dialog
Ring buffer with 2	
Stop capture after 1 tile(s)	Name Resolution
Stop Capture	Enable MAC name resolution
I after 1 packet(s)	Enable network name resolution
I after 1 megabyte(s)	
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!

₩ Ø ₩ ₩ ⊡	X 2 ⊟ Q + +		. 🖭 🕯	🖬 🗹 🖪 💥 🛙 🛱	
- Time	•				
- Time		Expression Clear_ Apply		[
1.0.000000	Source	Destination	Protocol	Info	
2 0.174052	e0:69:95:12:cd:15	Broadcast	ARP	Who has 140.78.100.141? Tell 140.78.100.174 Who has 140.78.100.138? Tell 140.78.100.212	
3 0.579412	HewlettP_c9:64:72	Spanning-tree-(for-br	STP	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_/6:De:36	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174 who has 140.78.100.1387 Tell 140.78.100.129	
7 2.158932	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
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-br	STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
10 2.854583	140 78 100 211	140 78 100 140	TCMP	Who has 140.78.100.138? TETT 140.78.100.129 Echo (ning) request	
12 3.150553	140.78.100.140	140.78.100.211	ICMP	Echo (ping) request	
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	
16 4 580183	e0:69:95:12:Cd:15	Spapping_tree_(for_br	STP	Who has 140.78.100.138? Tell 140.78.100.212	
17 5.149709	140.78.100.211	140.78.100.140	ICMP	Echo (pina) 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 6.1/4206	e0:69:95:12:Cd:15	Spanning_tree_(for_br	STP	Who has 140.78.100.138? Tell 140.78.100.212 RST Root = 32768/100/00:23:34:56:76:00 Cost = 220008 Rort = 0x800e	
					-
rame 8 (74 bytes on wi	re, 74 bytes captured)				
Arrival Time: May 18,	2012 13:02:17.726145000	200d-1			
ITIME delta trom prev	vious captured frame: 0.001149	000 seconds]			
[Time delta from prev	/ / / / / / / / / / / / / / / / / / / /	aooo seconasj			
[Time delta from prev [Time since reference	or first frame: 2 160081000	oconds]			
[Time delta from prev [Time since reference Frame Number: 8	or first frame: 2.160081000	seconds]			
[Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte	e or first frame: 2.160081000	seconds]			
[Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by	e or first frame: 2.160081000	seconds]			
[Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by [Frame is marked: Fal	se or first frame: 2.160081000 rtes se]	seconds]			
[Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte [Frame is marked: Fal [Protocols in frame:	se of first frame: 2.160081000 se tes se] eth:ip:icmp:data]	seconds]			
[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:	se or first frame: 2.160081000 settes [se] eth:ip:icmp:data] ICMP]	seconds]			
[Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String	<pre>cor first frame: 2.160081000 set tes tes tet:ip:icmp:data] icMP] ; icmp icmpv6]</pre>	seconds]			
Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String chernet II, Src: 20:76	e or first frame: 2.160081000 se se tes se] eth:ip:icmp:data] ICMP] : icmp icmpv6] ::8a:3e:a0:e2 (2c:76:8a:3e:a0:	seconds] e2), Dst: IntelCor_e9:2d	:7f (00	9:13:20:e9:2d:7f)	
Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte Capture Length: 74 by [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String chernet II, Src: 2c:76	<pre>cor first frame: 2.160081000 set tes se] eth:ip:icmp:data] ICMP] p: icmp icmpv6] ;:8a:3e:a0:e2 (2c:76:8a:3e:a0:1 140.78.100.140 (140.78.100.1</pre>	seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211	:7f (00 (140.7	9:13:20:e9:2d:7f) 8.100.211)	
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 thernet II, Src: 2c:76 tternet Protocol, Src: tternet Control Message	<pre>cor first frame: 2.160081000 set fres se] eth:ip:icmp:data] ICMP] : icmp icmpv6] ::8a:3e:a0:e2 (2c:76:8a:3e:a0:1 140.78.100.14 pe Protocol</pre>	seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211	:7f (00 (140.7)	9:13:20:e9:2d:7f) 8.100.211)	
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 thernet II, Src: 2c:76 thernet Protocol, Src: thernet Control Message	<pre>cor first frame: 2.160081000 ss ftes 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 pe Protocol</pre>	seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211	:7f (00 (140.7)	0:13:20:e9:2d:7f) 8.100.211)	_
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 [Protocols in frame: [Coloring Rule Name: [Coloring Rule String thernet II, Src: 2c:76 tternet Protocol, Src: nternet Control Messag	<pre>cor first frame: 2.160081000 ss ftes se] eth:ip:icmp:data] ICMP] i: icmp icmpv6] i:8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.14) pe Protocol</pre>	e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211	:7f (00 (140.7)	9:13:20:e9:2d:7f) 8.100.211)	_
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 [Protocols in frame: [Coloring Rule Name: [Coloring Rule String thernet II, Src: 2c:76 nternet Protocol, Src: nternet Control Messag	<pre>cor first frame: 2.160081000 sec or first frame: 2.16008100 sec or first frame: 2.1600810 sec or first frame: 2.16008100 sec or first frame: 2.1600810 sec or first fram</pre>	<pre>seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211</pre>	:7f (00 (140.7)	9:13:20:e9:2d:7f) 8.100.211)	
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 internet Protocol, Src: internet Control Messag	c or first frame: 2.160081000 sor first frame: 2.160081000 sse] eth:ip:icmp:data] ICMP] p: icmp icmpv6] i:8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1) p: Protocol c 76 8a 3e a0 e2 08 00 45 00 0 01 8e 69 8c 4e 64 8c 8c 4e	seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211 ,E. ,E.	:7f (00 (140.7;	9:13:20:e9:2d:7f) 8.100.211)	
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 thernet II, Src: 2c:76 nternet Protocol, Src: nternet Control Messag	c or first frame: 2.160081000 sc or first frame: 2.160081000 sc tes se] eth:ip:icmp:data] ICMP] sc icmp icmpv6] sc a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1- pe Protocol c 76 8a 3e a0 e2 08 00 45 00 0 01 8e 69 8c 4e 64 8c 8c 4e 0 01 00 1b 61 62 63 64 65 66	<pre>seconds] e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211EEEE</pre>	:7f (00 (140.7)	0:13:20:e9:2d:7f) 8.100.211)	
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 [Protocols in frame: [Coloring Rule Name: [Coloring Rule String thernet II, Src: 2c:76 nternet Protocol, Src: nternet Control Message 00 13 20 e9 2d 7f 2 00 3c 0a 5c 00 00 4 64 d3 00 00 55 40 0 67 68 69 6a 6b 6c 6	c 76 8a 3e a0 e2 08 00 45 00 c 76 8a 3e a0 e2 08 00 45 00 c 76 8a 3e a0 e2 08 00 45 00 c 76 8a 3e a0 e2 73 74 75 76	e2), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211 	:7f (00 (140.7)	9:13:20:e9:2d:7f) 8.100.211)	
Time delta from prev [Time delta from prev [Time since reference Frame Number: 8 Frame Length: 74 byte [apture Length: 74 byte [Frame is marked: Fal [Protocols in frame: [Coloring Rule Name: [Coloring Rule String hernet II, Src: 2c:76 iernet Protocol, Src: iernet Control Message 00 13 20 e9 2d 7f 2 00 3c 0a 5c 00 00 4 64 d3 00 00 55 40 0 67 68 69 6a 6b 6c 6	c 76 8a 3e a0 e2 08 00 45 00 c 76 8	<pre>seconds] 22), Dst: IntelCor_e9:2d 40), Dst: 140.78.100.211</pre>	:7f (00 (140.7)	9:13:20:e9:2d:7f) 8.100.211)	

Wireshark Ping

Intel(R) PRO/100 VE Network Co File Edit View Go Capture Ar	nnection - Wireshark alyze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp			<u></u>
] 🗶 🔁 占 🔍 🗢 🔿 🏹	<u>₽</u> □ □ 0 , Q	0	🎬 🗹 🍢 % 🙀
ilter:	•	Expression Clear Apply		
No Time	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	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 STP	RST. Root = 32768/100/00:23:34:56:76:00 Cost = 220008 Port = 0x800e
4 0.864438	Intel_40:e1:00	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129
6 1 854523	Intel_/0.be.so	Broadcast		who has 140.78.100.141: Tell 140.78.100.174
7 2.158932	140.78.100.211	140, 78, 100, 140	ICMP	Echo (pina) request
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-	br STP	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	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
14 4 150602	140.78.100.211	140.78.100.140	TCMP	Echo (ping) request
15 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.1382 Tell 140.78.100.212
16 4.580183	HewlettP c9:64:72	Spanning-tree-(for-	br STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 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? Tell 140.78.100.212
20 6.174206	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? 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
Ethernet II, Src: 2c:7 □ Destination: IntelCo	6:8a:3e:a0:e2 (2c:76:8a:3e:a0: r_e9:2d:7f (00:13:20:e9:2d:7f)	e2), Dst: IntelCor_e9:	2d:7f (00	0:13:20:e9:2d:7f)
Address: IntelCor_	e9:2d:7f (00:13:20:e9:2d:7f)			
0	= IG bit: Individu	al address (unicast)		
0	= LG bit: Globally	unique address (facto	ory defaul	lt)
■ Source: 2c:76:8a:3e:	a0:e2 (2c:76:8a:3e:a0:e2)			
Address: 2c:76:8a:	3e:a0:e2 (2c:76:8a:3e:a0:e2)			
0	= IG bit: Individu	al address (unicast)		
0	= LG bit: Globally	unique address (facto	ry defaul	lt)
Type: IP (0x0800)	-		-	
Internet Protocol. Src	: 140.78.100.140 (140.78.100.1	40), Dst: 140.78.100.2	11 (140.7	78.100.211)
Internet Control Messa	ae Protocol		(
	ge			
00 00 13 20 e9 2d 7f	C 76 8a 3e a0 e2 08 00 45 00	- V > F		
LO 00 3c 0a 5c 00 00 4	0 01 8e 69 8c 4e 64 8c 8c 4e	.<.\@i.NdN		
20 64 d3 00 00 55 40 0	0 01 00 1b 61 62 63 64 65 66	du@abcdef		
30 67 68 69 6a 6b 6c 6	6 6 6 6 70 71 72 73 74 75 76	ghijklmn opqrstuv		
IU // 01 02 03 04 65 0	0 0/ 08 09	wabcderg hi		
Source Hardware Address (eth.src), 6	5 bytes Packets: 21 Displayed: 21 Marked	0 Dropped: 0		Profile: Default

	🗙 🔁 占 🔍 🗢 🔿 🏹		2 🖂 🕯	🧸 🗹 幆 🔆 💢	
Filter:	•	Expression Clear Apply			
No Time	Source	Destination	Protocol	Info	<u>^</u>
1 0.000000 2 0.174052	Intel_76:be:36 e0:69:95:12:cd:15	Broadcast Broadcast	ARP	Who has 140.78.100.141? Tell 140.78.100.174 Who has 140.78.100.138? Tell 140.78.100.212	
3 0.579412	HewlettP_c9:64:72	Spanning-tree-(for-br	STP	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	
6 1.854523	Intel 40:e1:0d	Broadcast	ARP	who has 140.78.100.141? Tell 140.78.100.174 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	
8 2.160081	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
10 2.854583	Intel 40:e1:0d	Broadcast	ARP	who has $140.78.100.138$? Tell $140.78.100.129$	
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	
14 4.150692	140.78.100.211	140.78.100.140	TCMP	Echo (ping) request	
15 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
16 4.580183	HewlettP_c9:64:72	Spanning-tree-(for-br	STP	RST. Root = 32768/100/00:23:34:56:7c:00 Cost = 220008 Port = 0x800e	
1/ 5.149/09	140.78.100.211	140.78.100.140	TCMP	Echo (ping) request	
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	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
21 6.590423	HewTettP_C9:64:72	Spanning-tree-(for-br	STP	RSI. ROOT = 32/68/100/00:23:34:56:/C:00 COST = 220008 POPT = 0X800e	
					<u>×</u>
E Ethernet II. Src: 2c:76	8a:3e:a0:e2 (2c:76:8a:3e:a0)	e2). Dst: IntelCor e9:2d	1:7f (00	13:20:e9:2d:7f)	
Internet Protocol, Src:	140.78.100.140 (140.78.100.1	40), Dst: 140.78.100.211	(140.78	3.100.211)	
Version: 4	、			······	
Header length: 20 byte	25				
🗉 Differentiated Service	es Field: 0x00 (DSCP 0x00: De	fault; ECN: 0x00)			
Total Length: 60					
Identification: 0x0a5c	(2652)				
- Flags: 0x00	Not Sat				
<pre>0 = keserved blt: 0 = Dop't fragment</pre>	NOL SEL				
0 = More fragments	Not Set				
Fragment offset: 0	Not bet				
Time to live: 64					
Protocol: ICMP (0x01)					
Header checksum: 0x8e6	69 [correct]				
Source: 140.78.100.140	(140.78.100.140)				
Destination: 140.78.10	0.211 (140.78.100.211)				
Internet Control Message	Protocol				
000 00 13 20 e9 2d 7f 2c	76 8a 3e a0 e2 08 00 45 00				
010 00 3c 0a 5c 00 00 40	01 8e 69 8c 4e 64 8c 8c 4e	.<.\			
020 64 d3 00 00 55 40 00	01 00 1b 61 62 63 64 65 66	dU@abcdef			
030 67 68 69 6a 6b 6c 6d	6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv			

dit <u>Vi</u> ew <u>G</u> o <u>C</u> apture <u>A</u> n	alyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp			21 127 167 80 1 199	
		Expression Clear Apply	Q. III		
Time	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 0.1/4052	e0:69:95:12:cd:15	Spanning_tree_(for	ARP	Who has 140.78.100.138? Tell 140.78.100.212 RST_Root = 32768/100/00:23:34:56:76:00_cost = 220008_Root = 0x8000	
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	140.78.100.211	140.78.100.140	ICMP	Echo (ping) request	
9 2 579815	HewlettP c9:64:72	Spanning_tree_(for_	ar STP	RST Root = 32768/100/00.23.34.56.7c.00 Cost = 220008 Port = 0x800e	
0 2.854583	Intel_40:e1:0d	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.129	
1 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	
5 4.331539	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212	
6 4.580183	HewlettP_c9:64:72	Spanning-tree-(for-	or STP	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	
8 5.151104	140.78.100.140	140.78.100.211	ICMP	Echo (ping) reply	
9 5.1/4213	e0:69:95:12:cd:15	Broadcast	ARP	who has 140.78.100.138? Tell 140.78.100.212 who has 140.78.100.138? Tell 140.78.100.212	
1 6 500/22	Unilatep =0.64.73	Cooperating trees (for)	ar STP		
1 0. 090425	HewTettP_C9:64:72	spanning-tree-(for-i	01 011	RS1. ROOT = $32/68/100/00:23:34:56:7C:00$ COST = 220008 Port = 0.00000	
21 0.390423	HewTettP_C9:64:72	spanning-tree-(ror-i	51 511	RST. ROOT = 32/08/100/00:23:34:50:/C:00 COST = 220008 PORT = 0X800e	
21 0. 390423	HewTettP_C9:04:72	spanning-tree-(for-i	51 511	RSI. ROOT = 32/08/100/00:23:34:50:/C:00 COST = 220008 PORT = 0X800e	¥
me 8 (74 bytes on w	ire, 74 bytes captured)	spanning-tree-(ror-i		KSI. ROOT = 32/08/100/00:23:34:56:/C:00 COST = 220008 POPT = 0X800E	<u> </u>
ne 8 (74 bytes on w ernet II, Src: 2c:74	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0:</pre>	e2), Dst: IntelCor_e9:	2d:7f (00	<pre>kS1. R00t = 32/08/100/00:23:34:56:/C:00 Cost = 220008 Port = 0X800e :13:20:e9:2d:7f)</pre>	
ne 8 (74 bytes on w ernet II, Src: 2c:7 ernet Protocol, Src	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	•
ne 8 (74 bytes on w ernet II, Src: 2c:7 ernet Protocol, Src ernet Control Messa	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1 ge Protocol</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.78	<pre>kS1. Root = 32768/100/00:23:34:56:70:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
ne 8 (74 bytes on w ernet II, Src: 2c:7 ernet Protocol, Src ernet Control Messa ernet Control Messa ernet (Echo (ping)	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: 140.78.100.140 (140.78.100.1 ge Protocol reply)</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
ne 8 (74 bytes on w ernet II, Src: 2c:7 rrnet Protocol, Src ernet Control Messa ope: 0 (Echo (ping) ode: 0 ()	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply)</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.74	<pre>kS1. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
ne 8 (74 bytes on w ernet II, Src: 2c:74 ernet Protocol, Src ernet Control Messa rpe: 0 (Echo (ping) de: 0 () necksum: 0x5540 [con	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect]</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	4
ne 8 (74 bytes on w renet II, Src: 2c:7/ renet Protocol, Src renet Control Messay rpe: 0 (Echo (ping) ide: 0 () necksum: 0x5540 [con lentifier: 0x0001	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect]</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	4
ne 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa rpe: 0 (Echo (ping) ide: 0 () necksum: 0x5540 [con lentifier: 0x0001 quence number: 27	rrect] (0x001b)	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>RSI. ROOT = 32768/100/00:23:34:56:70:00 Cost = 220008 Port = 0x8000 :13:20:e9:2d:7f) 8.100.211)</pre>	4
ne 8 (74 bytes on w ernet II, Src: 2c:7 rnet Protocol, Src rnet Control Messau rpe: 0 (Echo (ping) ide: 0 () necksum: 0x5540 [con lentifier: 0x0001 quence number: 27 ta (32 bytes)	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b)</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32/08/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
e 8 (74 bytes on w ernet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa 'pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 quence number: 27 ta (32 bytes) Data: 6162636465666	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2</pre>	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32/08/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	T
e 8 (74 bytes on w rnet II, Src: 2c:74 rnet Protocol, Src rnet Control Messav /pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 67686996A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(ior-i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	T
e 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [coi entifier: 0x0001 quence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32768/100/00:23:34:56:70:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	1
e 8 (74 bytes on w rnet II, Src: 2c:7r rnet Protocol, Src rnet Control Messau pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	I
e 8 (74 bytes on w rnet II, Src: 2c:7r rnet Protocol, Src rnet Control Messar pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(ior-i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
e 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 quence number: 27 Data: 6162636465666 [Length: 32]	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32/08/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	I
<pre>le 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa pe: 0 (Echo (ping) de: 0 () eecksum: 0x5540 [con entifier: 0x0001 equence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]</pre>	<pre>rewitetP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32768/100/00:23:34:56:70:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	1
e 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messau pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con lentifier: 0x0001 quence number: 27 ita (32 bytes) Data: 6162636465666 [Length: 32]	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(() 0 - 4 e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>kS1. R00t = 32/08/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
he 8 (74 bytes on w ernet II, Src: 2c:7 ernet Protocol, Src ernet Control Messau ode: 0 () hecksum: 0x5540 [con lentifier: 0x0001 equence number: 27 ata (32 bytes) Data: 6162636465666 [Length: 32]	<pre>ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475</pre>	<pre>spanning-tree-(() of -4 e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761</pre>	2d:7f (00 11 (140.7)	<pre>RSI. ROOT = 32/68/100/00:23:34:56:/C:00 COST = 220008 POPT = 0X800E :13:20:e9:2d:7f) 8.100.211)</pre>	
ne 8 (74 bytes on w ernet II, Src: 2c:7r ernet Protocol, Src ernet Control Messar ope: 0 (Echo (ping) ode: 0 () necksum: 0x5540 [con entifier: 0x0001 equence number: 27 ita (32 bytes) Data: 6162636465660 [Length: 32]	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475	e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	I
ne 8 (74 bytes on w ernet II, Src: 2c:7 irnet Protocol, Src irnet Control Messa pe: 0 (Echo (ping) ide: 0 () necksum: 0x5540 [con lentifier: 0x0001 equence number: 27 ita (32 bytes) Data: 6162636465666 [Length: 32] 0 13 20 e9 2d 7f 2 0 3c 0a 5c 00 00 4	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761</pre>	2d:7f (00 11 (140.7)	RSI. ROOT = 32768/100/00:23:34:56:70:00 COST = 220008 POPT = 0X8002 :13:20:e9:2d:7f) 8.100.211)	T
<pre>he 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messau pe: 0 (Echo (ping) ide: 0 () ecksum: 0x5540 [con lentifier: 0x0001 guence number: 27 ita (32 bytes) Data: 6162636465666 [Length: 32]</pre>	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 E. E. </pre>	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
<pre>le 8 (74 bytes on w rnet II, Src: 2c:7r rnet Protocol, Src rnet Control Messar pe: 0 (Echo (ping) de: 0 () ecksum: 0x5540 [con entifier: 0x0001 quence number: 27 ta (32 bytes) pata: 6162636465660 [Length: 32]</pre>	rre, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 677777777777777777777777777777777777	<pre>spanning-tree-(ior-a e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 du@abcdef ghijklmn opgrstuv</pre>	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
he 8 (74 bytes on w rnet II, Src: 2c:7 rnet Protocol, Src rnet Control Messa rpe: 0 (Echo (ping) ide: 0 () lecksum: 0x5540 [col lentifier: 0x0001 equence number: 27 ita (32 bytes) Data: 6162636465666 [Length: 32] 0 13 20 e9 2d 7f 2 0 3c 0a 5c 00 00 4 54 d3 00 00 55 40 0 7 68 69 6a 6b 6c 6 7 61 62 63 64 65 6	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 777777777777777777777777777777777	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 du@abcdef ghijfimn opgrstuv wabcdefg hi</pre>	2d:7f (00 11 (140.7)	RSI: ROOT = 32768/100/00:23:34:56:70:00 COST = 220008 POPT = 0X8002 :13:20:e9:2d:7f) 8.100.211)	T
he 8 (74 bytes on w ernet II, Src: 2c:7 rrnet Protocol, Src ernet Control Messau pe: 0 (Echo (ping) ode: 0 () hecksum: 0x5540 [con lentifier: 0x0001 guence number: 27 tta (32 bytes) Data: 6162636465666 [Length: 32]	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 776 8a 3e a0 e2 08 00 45 00 0 0 1 8e 69 8c 4e 64 8c 8c 4e 0 0 1 0 0 1b [61 62 63 64 65 66 66 67 68 69	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 767761 0(@i.NdN d(@i.Nd.N d(@i.Nd.N d(@i.Nd.Cef ghijklmn opgrstuv wabcdefg hi</pre>	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
<pre>le 8 (74 bytes on w menet II, Src: 2c:7 met Protocol, Src met Control Messai pe: 0 (Echo (ping) de: 0 () lectsum: 0x5540 [col lentifier: 0x0001 quence number: 27 ta (32 bytes) Data: 6162636465666 [Length: 32]</pre>	<pre>rewTettP_C9:04:72 ire, 74 bytes captured) 6:8a:3e:a0:e2 (2c:76:8a:3e:a0: : 140.78.100.140 (140.78.100.1 ge Protocol reply) rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696 676869 6769 67</pre>	<pre>2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 76e. </pre>	2d:7f (00 11 (140.7)	<pre>kSi. Root = 32/68/100/00:23:34:56:/C:00 Cost = 220008 Port = 0x800e :13:20:e9:2d:7f) 8.100.211)</pre>	
<pre>ie 8 (74 bytes on w ernet II, Src: 2c:7 irnet Protocol, Src: irnet Control Messa rpe: 0 (Echo (ping) ide: 0 () iecksum: 0x5540 [con ientifier: 0x0001 equence number: 27 ita (32 bytes) Data: 6162636465666 [Length: 32]</pre>	rrect] (0x001b) 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475 6768696A6B6C6D6E6F707172737475	<pre>spanning-tree-(() of -i e2), Dst: IntelCor_e9: 40), Dst: 140.78.100.2 767761 767761 du@abcdet ghijfilm opgrstuv wabcdefg hi</pre>	2d:7f (00 11 (140.7)	RSI: ROOT = 32768/100/00:23:34:56:70:00 COST = 220008 POPT = 0X8002 :13:20:e9:2d:7f) 8.100.211)	T

Wireshark HTTP - DNS

-OX

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

<u>File Edit View Go Capture Analyze Statistics Telephony Tools Help</u>

Packets: 346 Displayed: 346 Marked: 0 Dropped: 0

Filter:		▼ E	Expression Clear Apply			
No	Time	Source	Destination	Protocol	Info	[_
/	1.698687	74.125.232.239	140.78.100.211	TCP	nttps > 8462 [ACK] Seq=1 ACK=2 W1N=257 Len=0 SLE=1 SRE=2	1
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 MS5=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	
1/	2.436639	140./8.100.211	65.52.107.149	тср	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	2
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	4
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 MS5=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	тср	http > 8648 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=2	
J 30	2.996742	140.78.100.211	193.170.140.71	тср	8648 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0	_
B Ether E Inter Domai Domai Fla Que Ans Aut Add Que N N N N N N N N N N N N N	net Protocol, Src: 140.78.1 Datagram Protocol, Src Port n Name System (query) <u>sponse In: 9</u>] nsaction ID: 0x005f gs: 0x0100 (Standard query) stions: 1 wer RRs: 0 hority RRs: 0 itional RRs: 0 ries ww.bing.at: type A, class I Name: www.bing.at Type: A (Host address) class: IN (0x0001)	:N), Dst: 140.78.100.11 Port: domain (53)	9 (140.78	8.100.119)	
0000 00 0010 00 0020 64 0030 00 0040 6	0 07 e9 40 e1 0d 00 13 20 0 39 2b 6b 00 00 80 11 2d 4 77 d3 f6 00 35 00 25 94 0 00 00 00 00 00 03 77 77 1 74 00 00 01 00 01	e9 2d 7f 08 00 45 00 62 8c 4e 64 d3 8c 4e fb 00 5f 01 00 00 01 77 04 62 69 6e 67 02	@E. .9+kb.NdN dwwww.bing. at			

O Text item (), 17 bytes

Michael Sonntag

Profile: Default

Wireshark HTTP - DNS

F		M		
	📶 Intel(R) PRO/100 VE Netw	ork Connection -	Wireshark

Eile Edit View Go Capture Analyze Statistics Telephony Tools Help

🗀 🗔 🗶 😂 占 | 의, 수 수 😜 🛜 👱 | 🗐 📑 | 연, 인, 인, 🗹 | 🖉 🕵 % | 🔀 01

Filter:		▼ 8	E <u>x</u> pression Clea <u>r</u> App <u>l</u> y			
No	Time	Source	Destination	Protocol	Info	
1	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	1
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	1
10	2.035153	140.78.100.211	140.78.100.119	DNS	Standard query AAAA www.bing.at	
11	2.315300	140.78.100.119	140.78.100.211	DNS	Standard query response	
12	2.310310	140.78.100.211	65 52 107 149	TCP	0044 > ILLP [STN] Seq=0 WIN=0192 [EIN=0 MSS=1400 WS=0	
14	2.310040	65 52 107 1/9	140 78 100 211	TCP	0045 > 1000 [SIN] Seq-0 with 0192 Left with 354 400 ws-0 mss-1460 ws-0	
15	2 436499	140 78 100 211	65 52 107 149	TCP	8644 > http [44	
16	2,436609	65, 52, 107, 149	140, 78, 100, 211	TCP		
17	2,436639	140.78.100.211	65, 52, 107, 149	TCP	8645 > http ind What's this? Investigate	
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 Mg	
20	2.609521	140.78.100.211	140.78.100.119	DNS	Standard guery	
21	2.791682	Intel_40:e1:0d	Broadcast	ARP	who has 140.78. Noto: Coogle Chrome used	
22	2.791711	Intel_40:e1:0d	Broadcast	ARP	who has 140.78. NOLE. GOOGLE CHIOHE USED	
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 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	193.1/0.140./1	тср	8648 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8	
28	2.993682	140.78.100.211	193.1/0.140./1	TCP	8649 > nttp [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=8	
29	2.990085	193.1/0.140./1	140.78.100.211	TCP	HLP > 8048 [SYN, ACK] Seq=0 ACK=1 WIN=14000 Len=0 MSS=1400 WS=2	
50	2.990742	140.78.100.211	193.1/0.140.71	ICF	SOUR A LEFT ACK I WITH STAR FEIL	
+ User	Datagram Protocol, Src Port	t: domain (53), Dst Por	rt: 54262 (54262)			
- Domai	n Name System (response)					
[Re	nuest In: 8]					
[Ti	no: 0.284202000 soconds]					
ira	nsaction ID: 0x005F					
🕀 Fla	gs: 0x8400 (Standard query	response, No error)				
Que	stions: 1					
Ans	wer RRs: 1					
Aut	hority RRs: 0					
Add	itional RRs: 0					
	ries					
	vers					
	ww.bing.at: type A. class i	IN. addr 65.52.107.149				
	Name: www.bing.at					
	Type: A (Host address)					
	class: TN (0x0001)					
	Time to live: 1 hour					
	Data length: 4					
	Adda, 65 52 107 140					_
	Auur: 05.52.10/.149					Ψ.

	Dat Add	al Ir:	eng 65.	th: 52.	4 107	.14	9								
0000 0010 0020 0030 0040 0050	00 13 00 49 64 d3 00 01 61 74	20 69 00 00 00 00	e9 9b 35 00 00 41	2d 00 d3 00 01 34	7f 00 f6 00 00 6b	00 7f 00 03 01 95	07 11 35 77 C0	e9 f0 25 77 0c	40 21 5f 77 00	e1 8c 00 04 01	0d 4e 5f 62 00	08 64 84 69 01	00 77 00 6e 00	45 8c 00 67 00	00 4e 01 02 0e

00	13	20	e9	2d	7f	00	07	e9	40	e1	0d	08	00	45	00				.@	Ε.
00	49	69	9b	00	00	7f	11	f0	21	8c	4e	64	77	8c	4e		.Ii		. ! . Ndv	1. N
64	d3	00	35	d3	f6	00	35	25	5f	00	5f	84	00	00	01		d 5.	5	%	
00	01	00	00	00	00	03	77	77	77	04	62	69	6e	67	02			w	ww.bir	ıa.
61	74	ōō	ōō	01	00	01	c0	00	00	01	00	01	00	00	0e		at			
10	00	04	41	34	6b	95											A4	k.		
item (0 16	byte	e.						Pad	rete:	3461	Dienla	wed	346	Mark	ed.	0 Dropp	o -be		
ochin y	0, 10								1.00		0.001	Jispic	ycu.	0.0	1-101110	cu.	o Di oppi			

Text item (), 16 bytes

Profile: Default

Wireshark HTTP - Request

Image: Project Proj (V) If Michael Connections Windowski Image: Proj Proj Proj Proj Proj Proj Proj Proj	<u>"</u>]~/					HTTP - Red
Ib Ext Verm 6 Capetan Levine Verm 7 Ext Verm 6 Capetan Levine Verm 7 Im State The State State The State The State State The State	📶 Intel(R) PRO/100 VE Netwo	rk Connection - Wireshark				
Image: Image:<	<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	e <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp)			
The: Top Source Destination Probability 11 2.315500 140,78.100.211 0.40,78.100.211 <th>🖼 🕍 😂 🚳 🕷 E</th> <th>8 🖬 🗶 😂 占 🔍 🗢 🧼 🥥</th> <th>77 🕹 🔳 📑 €, €</th> <th>0 🖭 1</th> <th>¥ 🗹 🍢 % 💢</th> <th></th>	🖼 🕍 😂 🚳 🕷 E	8 🖬 🗶 😂 占 🔍 🗢 🧼 🥥	77 🕹 🔳 📑 €, €	0 🖭 1	¥ 🗹 🍢 % 💢	
Inc. Inc. Source Destination Product Mode Mode 11 22:15:00 140.78.100.211 35.78.100.211 97.78.100.213 97.78.100.213 97.78.100.213 97.78.100.	Filter:		▼ Expression Clear Apply			
1 2:33500 140.78.100.211 five 5tandard query response 1 2:33500 140.78.100.211 five 8644 > http [sv), sell seed withel32 Lend NSS-1400 wesd 1 2:43635 65.32.107.149 five 65.32.107.149 five 8644 > http [sv), sell seed withel32 Lend NSS-1400 wesd 1 2:43656 65.32.107.149 five five 8644 > http [sv), sell seed withel330 Lend NSS-1400 wesd 1 2:436669 65.32.107.149 140.78.100.211 five 8644 > http [sv), sell seed withel330 Lend NSS-1400 wesd 1 2:436669 65.32.107.149 140.78.100.211 five NSS-1400 wesd 1 2:436669 65.32.107.149 140.78.100.211 five http [sv], sell seed withel330 Lend NSS-1400 wesd 1 2:436669 65.32.107.149 140.78.100.211 five seed withel32 Lend NSS-1400 wesd 1 2:436669 140.78.100.211 five seed withel32 Lend NSS-1400 wesd seed withel330 Lend NSS-1400 wesd 2:2:787171 100.78.00.211 five seed withel330 Lend NSS-1400 wesd seed withel330 Lend NSS-1400 wesd 2:2:77771 100.78.00.211 five seed withel330 Lend NSS-1400 wesd seed withel330 Lend NSS-140	No Time	Source	Destination	Protocol	Info	
11 2.13638 140.78.100.211 05.22.107.139 TCP Set3 Mines022 Letrol MSS-1400 MSS-1 12 2.436439 140.78.100.211 TCP Mttp Set4 Mines022 Letrol MSS-1400 MSS-1 12 2.436439 140.78.100.211 TCP Mttp Set4 Mines022 Letrol MSS-1400 MSS-0 12 2.436439 140.78.100.211 TCP Mttp Set4 Mines022 Letrol MSS-1400 MSS-0 13 2.436439 140.78.100.211 TCP Set4 Mines022 Letrol MSS-1400 MSS-0 13 2.436439 140.78.100.211 GS.22407410 Mttp Mttp Mines022 Letrol MSS-1400 MSS-0 14 2.436439 140.78.100.211 140.78.100.211 Mttp Mttp Mines022 Letrol MSS-1400 MSS-0 14 2.436439 140.78.100.211 140.78.100.211 Mttp Mttp Mttp Mines022 Letrol MSS-1400 MSS-0 14 2.436439 140.78.100.211 Mttp <	11 2.315500	140.78.100.119	140.78.100.211	DNS	Standard query response	
14 2:43335 65:32:107:149 140:78:100:211 TCP Pttp	12 2.316318	140.78.100.211	65.52.107.149	TCP	8644 > http [SYN] Seq=0 Wi 8645 > http [SYN] Seq=0 Wi	n=8192 Len=0 MSS=1460 WS=8 n=8192 Len=0 MSS=1460 WS=8
115 2.438499 140.76.100.211 65.52.107.149 TCP 804.74.100.74.100.74.100.75.100.74.100 Http: > 805.710, Ackg steep-0 Http: > 805.710, Ackg steep-0 115 2.438499 140.76.100.211 TCP Bit Ackg steep-0 Http: > 805.710, Ackg steep-0 Http: > 805.710, Ackg steep-0 118 2.438497 140.76.100.211 140.76.100.211 HTTP: GGT / HTTP/11 HTTP: GGT / HTTP/11 Http: > 805.7100.413 Ht	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
10 2.32,10/.149 140,78.100,211 TCP REP 864 5 SYM, ACK J Sequed Ack-L Wine-3300 Len-0 13 2.403927 110,78.100,211 65.32.10/.149 140.78.100,211 PTCP REP & Standard Rep- & Standa	15 2.436499	140.78.100.211	65.52.107.149	TCP	8644 > http [ACK] Seq=1 Ac	k=1 win=65536 Len=0
Iter a results Iter	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
192.60531 140.75.100.211 HTTP	1/ 2.430039	140.78.100.211	65. 52. 107. 149	НТТР	GET / HTTP/1_1	K=1 WIN=00000 Len=U
20 2:	19 2.603541	65. 52. 107. 149	140.78.100.211	нттр	HTTP/1.1 301 Moved Permane	ntly
12.2/3052 Intel_40:e1:0d Broadcast APP Who has 140.78.100.1417 Tell 2 :/yoprtext Transfer Protocol Broadcast APP Who has 140.78.100.1417 Tell B :GFT / HTP/1.1V/n Bit Start Frein Broadcast APP Who has 140.78.100.1417 Tell Request URE: (Figure 11/6) Bit Start Frein Broadcast APP Who has 140.78.100.1417 Tell Request URE: (Figure 11/6) Bit Start Frein Broadcast APP Who has 140.78.100.1417 Tell Connection: Kepust URE: (Figure 11/6) Bit Start Frein Bit Start Frein <td>20 2.609521</td> <td>140.78.100.211</td> <td>140.78.100.119</td> <td>DNS</td> <td>Standard query A www.bing.</td> <td>com</td>	20 2.609521	140.78.100.211	140.78.100.119	DNS	Standard query A www.bing.	com
21 £ 1.73114 INCET_2V.41.00 DF VAULASL APP WHO HAS 140.75100.138: TET VVNAL ARE (NESS ? INVESS B geptext Transfor Protocol B (Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n] Request Version: HTTP/1. Request Version: HTTP/1. Host: www.bing.at/r\n Connection: keep-alive/r\n Connection: keep-alive/r\n Status in a polication/xhtml+xml, application/xhtml+xml, application/xhtml+x	21 2.791682	Intel_40:e1:0d	Broadcast	ARP	Who has 140.78.100.141? T	
<pre>E Hyper Lett. Trains Hy rotation E Hyper Lift. (Chat/Sequence): GET / HTTP/L1\r\n] Request Wethod: GET Request VerSion: HTTP/L1.1 Host: www.bing.at/r\n connection: keep-alive/r\n User-Agent: Mozilla/5.0 (windows NT 6.1; WoW64) Applewebkit/535.19 (kHML, like Gecko) Chrome/18.0.1025.168 Safari/535.19\r\n Accept: text/Thml.application/kHml+xml, application/xml;q=0.9,*/*;q=0.8\r\n Accept: text/Thml.application/kHml+xml, application/xml;q=0.9,*/*;q=0.8\r\n Accept: Lext/Thml.application/kHml+xml, application/kHml+xml, applica</pre>		Inter_40.e1.00	broadcast	AKP	and has 140.70.100.138? 1	🚆 what are these? Inve
<pre>b [Expert Into (Chat/Sequence): GaT / HIP/1.1(r(h) Request Version: HTTP/1.1 Host: www.bing.att/r)n Connection: keep-aliver/n user-Agent: Mozilla/S.0 (windows T6.1; wow64) Applewebkit/535.19 (kHTML, like Gecko) Chrome/18.0.1025.168 safari/535.19\r/n Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml.application/xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.application/xhtml+Xml;q=0.9,*/*;q=0.8\r/n Accept:text/html.applicatio</pre>	GET / HTTP/1.1\r		-)]			
0010 01 03 20 14 00 80 00 27 19 82 46 43 41 <						
	Request Version Request Version Host: www.bing.at Connection: keep- User-Agent: Mozi Accept: text/htmi Accept: text/htmi Accept-Encoding: Accept-Language: Accept-charset: 1 \r\n	h: HTTP/1.1 E\r\n -alive\r\n lla,5.0 (Windows NT 6.1; WoW64) l,application/xhtml+xml,applicat gzip,deflate,sdch\r\n de-DE,de;q=0.8,en-US;q=0.6,en;c tso-8859-1,utf-8;q=0.7,*;q=0.3\r	ApplewebKit/535.19 (Кн tion/xml;q=0.9,*/*;q=0. q=0.4\r\n `\n	™L, like G 8\r\n	ecko) Chrome/18.0.1025.168 5a	afari/535.19\r\n

Wireshark HTTP - Response

	-M				vires	SN
ลไ					HTTP - Resp	or
·]	Totel(R) PRO/100 VE Network Conner	ction - Wireshark				
	File Edit View Go Capture Analyze	Statistics Telephony Tools Help				
		 ≰ ᢓ ⊟ 0,			M M 🕅 🎎 🕅	
	Filter:	•	Expression Clear Apply			
	No - Time	Source	Destination	Protocol	Info	
	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 W1n=4380 Len=0 MSS=1460 WS=0	
	18 2 427177	140.78.100.211	65 52 107 149		8045 > NTTP [ACK] SEGEL ACKEL WINE05530 LENEU	
	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 2.80/614	140.78.100.211	65.52.107.149 140.78.100.211	TCP	8644 > NTTP [ACK] Seq=396 ACK=302 W1n=65280 Len=0 Standard query response CNAME akam bing com CNAME a124]m akamai not A 16	2 17
		•				
	⊟ HTTP/1.1 301 Moved Perm	anently\r\n quence): HTTP/1.1 301 Moved /1.1	Permanent]y\r\n]			
	Cache-Control: no-cache Location: http://www.bi Edge-control: no-store\ P3P: CP="NON_UNT_COM_NA	\r\n ng.com/?cc=at\r\n Rec				
	Set-Cookie: HOP=T=1&TS	=1337341091: domain=.bing.a	t: $path=/(r)n$			
	Date: Eri, 18 May 2012	11:38:11 GMT\r\n				
	\Box Content-Length: 0\r\n					
	[Content length: 0]					
	\r\n					
			the second second			
	0020 64 d3 00 50 21 c4 b8 c	0 01 00 41 34 00 95 8C 4e	.u.Q@ aTA4KN			
	0030 12 a7 88 5d 00 00 48 5	54 54 50 2f 31 2e 31 20 33]HT TP/1.1 3			
	0040 30 31 20 4d 6f 76 65 6	4 20 50 65 72 6d 61 6e 65	01 Moved Permane			
	0050 6e 74 6c 79 0d 0a 43 6	63 68 65 2d 43 6f 6e 74	ntlyCa che-Cont			
	0070 6f 63 61 74 69 6f 69 3	20 03 01 03 08 03 00 00 00 4C	ocation: http://			
	0080 77 77 77 2e 62 69 6e 6	7 2e 63 6f 6d 2f 3f 63 63	www.bing .com/?cc			
	0090 3d 61 74 0d 0a 45 64 6	57 65 2d 63 6f 6e 74 72 6f	=atEdg e-contro			
	00a0 6c 3a 20 6e 6t 2d 73 7	4 6T 72 65 0d 0a 50 33 50	I: no-st oreP3P			
	00c0 4d 20 4e 41 56 20 53 5	54 41 20 4c 4f 43 20 43 4l	M NAV ST A LOC CU			
	00d0 52 61 20 44 45 56 61 2	20 50 53 41 61 20 50 53 44	Ra DEVa PSAa PSD			
	00e0 61 20 4f 55 52 20 49 4	le 44 22 0d 0a 53 65 74 2d	a OUR IN D"Set-			
	00T0 43 6T 6T 6D 69 65 3a 2	20 5T 48 4T 50 3d 49 3d 31	Cookie: _HOP=I=1			
	0110 64 6f 6d 61 69 6e 3d 2	20 53 34 31 30 39 31 30 20 2e 62 69 6e 67 2e 61 74 3b	domain=, bing_at.			
	0120 20 70 61 74 68 3d 2f 0	0d 0a 44 61 74 65 3a 20 46	path=/Date: F			
	0130 72 69 2c 20 31 38 20 4	d 61 79 20 32 30 31 32 20	ri, 18 M ay 2012			
	0140 31 31 3a 33 38 3a 31 3	20 47 4d 54 0d 0a 43 6f	11:38:11 GMTCo			
	0160 0a 0d 0a	oo oe o/ /4 o8 3a 20 30 0d	ntent-Le ngth: 0.			
	oros va ou va					-
	HTTP Set Cookie (http.set_cookie), 61 bvt	es Packets: 346 Displayed: 346 Mark	ed: 0 Dropped: 0		Profile: Default	
					I. Control Sector	11

Michael Sonntag

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

Wireshark HTTP - Stream

Follow TCP Stream	_ [
itream Content	
Jet / (Ceat nil//1.1	-
onnection: keep-alive	
Ser-Agent: Mozilla/5.0 (Windows NT 6.1: WOW64) ApplewebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.168	
afar 1/535.19	
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	
ccept-Encoding: gzip,deflate,sdch	
<pre>sccept-Language: _de-DE,de;q=0.8,en-US;q=0.6,en;q=0.4</pre>	
Accept-Charset: ISO-8859-1,utt-8;q=0.7,*;q=0.3	
1 1 200 ov	
ache Control: private max-age=0	
ontent-Type: text/html: charse=utf-8	
3P: CP="NON UNI COM NAV STA LOC CURA DEVA PSAA PSDA OUR IND"	
/ary: Accept-Encoding	
ontent-Encoding: gzip	
Date: Fri, 18 May 2012 11:38:11 GMT	
ontent-Length: 10051	
onnection: keep-alive	
et-Cookie: _FS=mkt=0e-Al@NU=1; 00matn=.Ding.com; patn=/	
set-cookie: MUTD=264E4596E1D561753E42046EEE0D26193: expires=Sun 18-May-2014 11:38:11 GMT: domain= bing com:	
ath=/	
et-Cookie: OrigMUID=264FA59BF1D561753F42A6FFF0D26193%2c5546792e35a8415997835740de96da67; expires=Sun, 18-	
Hay-2014 11:38:11 GMT; domain=.bing.com; path=/	
et-Cookie: sRCHD=D=2303258&MS=2303258&AF=NOFORM; expires=Sun, 18-May-2014 11:38:11 GMT; domain=.bing.com; pat	า=/
set-Cookie: SRCHUID=V=2&GUID=EFF4F73D88574A12B17D3F6371AEC69D; expires=Sun, 18-May-2014 11:38:11 GMT; path=/	
et-Cookie: SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20120518; expires=Sun, 18-May-2014 11:38:11 GMT; domain=.bing.com;	
atn=/	
IV8 FIdvaN HHB" X 5ab 3 @ 5.2 @ "@ AV	
B_{1} f $b/$ oI $d9h6w$ i $a4k$ $o~AX&6$ Di KNY BR $a7. > /$	••••
bw.0нh.x\$&~.v4d.8"5".z#y\воеR.wRr.l=.y~./.7ff.k.!8lnМА.	
Find Save As Print Entire conversation (113759 bytes)	🖲 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

A 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. gm. 2=. {.21h	ŧ. 👘
[3~.to'equv.}fq.]bs.)gDc^MH.?=.01.q}.d~	
\$Bl2.7@.9.gΓ.z2f.SAsc0r	
' Za.`	
(t.Edo#`*x.1m6C?8"i*8.P/MK.*.'/.8.v]i&L.	
%. :.M{^[.B. v.:m.%%[.1.92].eq9.b5.Pf.v".%p.5.r.Ky*.OMN#.Pk.7shiF.q.)	
n. /.e. >~=4. #0. YM. A. G. 4xi, EMS. i. kx. ir. i.fYP. [Et]. +Gi/"/	
· (C	
[/. Tx. 'fz	
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:g=0.8.en-U5:g=0.6.en:g=0.4	
Accept-Charset: ISO-8859-1.utf-8:g=0.7.*:g=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	
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	-
Eind Save As Print Entire conversation (113759 bytes)	Raw
Help Filter Out This Stream Clos	e

F

Wireshark HTTP authentication

Image: Control of Contro	- 1						
Interface of the second s	۱L	<u>I</u>				HTTP authentic	2
The Set You Go Quant You Want Section Technology Due 190 We de	Į,	Intel(R) PRO/100 VE Network Conne	ection - Wireshark				ļ
Image: Solution Image: Solution Image: Solution Image: Solution 13 6.054607 21.07.8.00.0211 21.8.05.05.00 100.001 13 6.054607 21.0.05.05.01 11.0.05.05.00 100.001 14 6.054607 21.0.05.05.01 11.0.001 100.001 100.001 14 6.054607 21.0.05.01 100.001 1	· [<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyz	ze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp				
Num: Personan Case, Kedy bs. The Source Destation Note: Note: <th></th> <th></th> <th>🗙 🔁 📇 🔍 🗢 👄 😜 🤅</th> <th>7 🕹 🔳 📑 🗨 G</th> <th>0 🖭 1</th> <th>🥻 🗹 畅 % 🧝</th> <th></th>			🗙 🔁 📇 🔍 🗢 👄 😜 🤅	7 🕹 🔳 📑 🗨 G	0 🖭 1	🥻 🗹 畅 % 🧝	
Nu. The Source Destends Proceed Proced	Ī	Filter: http		Expression Clear Apply			
136.684160 140.78.100.711 213.456.65.100 HTTP HTTP://1.30.10011 HTTP://1.30.100111 HTTP://1.30.10011	Ī	No. Time	Source	Destination	Protocol	Info -	
13.6.948697 21.3.85.85.100 30.78.00.211 HTP HTP2.1.302.Found (Text/Intl) 27.7.00223 22.3.165.64.7 140.78.100.211 HTP2.1.302.Found (Text/Intl) 27.7.00223 22.3.165.64.7 11.1.65.4.72 HTP2.1.302.Found (Text/Intl) 27.7.00223 22.3.165.64.7 12.1.65.4.72 HTP2.1.302.Found (Text/Intl) 27.7.00223 22.3.165.64.7 12.1.65.4.72 HTP2.1.302.Found (Text/Intl) 27.7.00223 22.3.165.64.7 12.1.65.4.72 HTP2.1.302.Found (Text/Intl) 27.7.2.204.172 12.0.7.0.0211 HTP2.1.177.1.100.Found (Text/Intl) 27.7.2.204.172 12.0.7.02.0211 HTP2.1.177.1.100.Found (Text/Int	Ĩ	13 6.804169	140.78.100.211	213.165.65.100	HTTP	POST /de/cgi/login HTTP/1.1 (application/x-www-form-urlencoded)	
19 59:0000 100:0000000000000000000000000000000000		15 6.945697	213.165.65.100	140.78.100.211	HTTP	HTTP/1.1 302 Found (text/html)	
12 7.05223 140.03.000.21 11777		19 0.985/09	212 165 64 71	213.103.04./1	HTTP	GET //Status=TogIn-Tatled HTP/I.I	
<pre>1 2 2:10001 1 213.105.41.72 1 140.75.100.211 213.105.41.72 mTTP GT //15.100 00* (rest./html) //15.101 1 213.105.41.71 mTTP //1.100 00* (rest./html) //15.101 1 213.105.41.71 mTTP //1.100 00* (rest./html) //15.101 //</pre>		25 7.058273	140, 78, 100, 211	213, 165, 64, 72	нттр	GET /?status=login-failed HTTP/1.1	
47 7.56804 140.75.100.211 213.165.64.72 HTTP GT /vim.html HTTP/1.1 13 7.59253 140.75.100.211 217.72.204.122 HTTP GT /vim.html HTTP/1.1 13 7.59253 140.75.100.211 217.72.204.122 HTTP GT /vim.ytml Strift 14 7.50243 140.75.100.211 217.72.205.200 HTTP GT /vim.ytml Strift 15 7.604422 217.72.205.200 HTTP HTTP/1.1 GT /vim.ytml Strift 16 Frame 13 (754 bytes on wire, 754 bytes captured) HTTP HTTP/1.1 GT /vim.ytml Strift Strift 17 Intermet Protocol, scr: 140.78.100.211 MtTP/1.1 HTTP HTTP/1.1 HTTP/1.1 16 Intermet Protocol, scr: 140.78.100.211 MtTP/1.1 HTTP/1.1 HTTP/1.1 17 Intermet Protocol, scr: 140.78.100.211 MtTP/1.1 HTTP/1.1 HTTP/1.1 16 Intermet Protocol, scr: 140.78.100.211 MtTP/1.1 HTTP/1.1 HTTP/1.1 18 Gtapin HTTP/1.1 HTTP/1.1 HTTP/1.1 HTTP/1.1 HTTP/1.1 19 Intermet Protocol, scr: HTP/1.1 HTTP/1.1		42 7.180847	213.165.64.72	140, 78, 100, 211	HTTP	HTTP/1.1 200 OK (text/html)	
50 7.597290 140.78.100.211 217.72.204.1/22 HTTP HTTP./1.1200 or (Kext/Html) 51 7.607270 213.656.64.22 140.78.100.211 HTTP HTTP./1.1200 or (Kext/Html) 53 7.650422 217.72.204.172 140.78.100.211 HTTP HTTP/II.1200 or (Kext/Html) 64 7.830421 217.72.204.172 140.78.100.211 HTTP HTTP/II.1200 or (Kext/Html) 64 7.830421 217.72.204.172 140.78.100.211 HTTP HTTP/II.1200 or (Kext/Html) 64 7.830421 140.78.100.211 (40.78.200.212) HTTP HTTP/II.1200 or (Kext/Html) 65 7.650422 217.72.204.122 HTTP HTTP/II.1200 or (Kext/Html) HTTP 66 7.850421 140.78.100.211 (40.78.200.212) HTTP HTTP/II.1200 or (Kext/Html) 67 7.850421 140.78.100.211 (40.78.200.212) HTTP HTTP/II.1200 or (Kext/Html) 68 For theorem or (10 protoc), src: 140.78.100.211 (40.78.200.211) HTTP HTTP/II.1200 or (Kext/Html) 69 For theorem or (10 protoc), src: 140.78.100.211 (40.76.01/0.011 HTTP/II.1200 HTTP/II.1200 60 For theorem or (10 protoc), src: 120 for (12.120, src) (21.10.10.111) HTTP/II.1200 HTTP/II.1200		47 7.568014	140.78.100.211	213.165.64.72	HTTP	GET /uim.html HTTP/1.1	
51 7.60270 213.165.64.72 140.78.100.211 HTTP HTTP Anticipation of the state of th		50 7.597259	140.78.100.211	217.72.204.172	HTTP	GET /ngvar.js HTTP/1.1	
527.63443 140,78.100,211 2.2.193,234 HTTP HTTP HTTP, L200 or (application/x-javascript) 527.63422 127.72.201,21 127.72.201,200 ntTP HTTP HTTP, HTTP,1200 or (application/x-javascript) 647.831935 140.84.100.211 217.72.201,200 ntTP HTTP HTTP, HTTP,1200 or (application/x-javascript) 647.831935 140.78.100.211 100.11120/e92/d277) DSt: Intel_40/e12/00 ntTP HTTP 767.840.00 St: intel_con_e92/d277 100.11120/e92/d277) DSt: Intel_40/e12/00 ntTP HTTP 8 Framemission control protocol, Src: 100.78:100.211 L00.11120/e92/d277) DSt: Intel_40/e12/00 Internet Protocol 9 DOT (MeQigi/Apoin HTTP/L1/N) E E E E E 9 DOT (MeQigi/Apoin HTTP/L1/N) E E E E E E 9 DOT (MeQigi/Apoin HTTP/L1/N) E		51 7.607270	213.165.64.72	140.78.100.211	HTTP	HTTP/1.1 200 OK (text/html)	
35 7,630422 217,72,74,172 140.78,1000.211 PTTP HTTP.1.1 200 OK (application/x-javascript) 6 7,831031 140.78,1000.211 217,72,203.230 HTTP HTTP.1.1 200 OK (application/x-javascript) 8 Frame 13 (734 bytes on wire, 734 bytes captured) 140.78,1000.211 217,72,203.230 140.78,1000.211 217.72,203.230 9 Transission Control Protocol, src: 1100,73,100.211 (201.72,000.210) DST infection/x-javascript) 150 9 Transission Control Protocol, src: 140.78,100.211 (201.72,000.210) DST infection/x-javascript) 150 9 Transission Control Protocol, src: 140.78,100.211 (201.72,000.210) DST infection/x-javascript) 150 9 Transission Control Protocol, src: 140.78,100.211 (201.72,000.210) DST infection/x-javascript) 150 9 DST infection/x-lavascript) DST infection/x-lavascript) 150 150 150 10 Content-length: 116/ Chack-control: 180 160/261/00jn 160 Request Wir/in 160 160 1100000000000000000000000000000000000		52 7.623443	140.78.100.211	2.21.93.234	HTTP	Continuation or non-HTTP traffic	
64 7,831915 140,78,100,211 217,72,203,250 HTP GET /7LooutAdProxX,SerViCe-htTristStite-amx8dection-amx/homepade/start/at/ 18 Finame 13 (756 bytes on wire, 756 bytes capued) Internet Protocol, Src: 140,78,100,211 (40,78,100,211), Dist: 213,165,5100) 19 Internet Protocol, Src: 140,78,100,211 (40,78,100,211), Dist: 213,165,5100) 10 Internet Protocol, Src: 140,78,100,211 (40,78,100,211), Dist: 213,165,5100) 11 Internet Protocol, Src: 140,78,100,211 (40,78,100,211), Dist: 213,165,5100) 12 IPOST /de/cgl//login HTTP/L.1/r\n 14 Expert Info (chat/Sequence): POST /de/cgl/login HTTP/L.1/r\n] Request us: /de/cgl/login Request Us: /de/cgl/login 13 Content-iength: 116/ 14 Content-iength: 116/ 15 Content-iength: 116/ 16 Content-iength: 116/ 17 Content-iength: 116/ 18 Content-iength: 116/ 19 Content-iength: 116/ 10 Content-iength: 116/ 10 Content-iength: 116/ 10 Content-iength: 116/ 10 Content-iength: 116/ 116 Content-iength: 116/ 117 Content-iength: 116/		55 7.630422	217.72.204.172	140.78.100.211	HTTP	HTTP/1.1 200 OK (application/x-javascript)	
<pre> Frame 13 (754 bytes on wire, 754 bytes captured) Ethernet II, Src: Inteloca-gid:7(00:13:10:69:20:7f), DSt: Intel_40:e1:0d (00:07:e9:40:e1:0d) Trainsission control Protocol, src: 140.78:100.211 (140.78:100.211), DSt: 213.165.65:100 (213.165.65:100) Trainsission control Protocol, src: Port: 12107 (21207), DSt Port: http (80), Seq: 1, Ack: 1, Len: 700 Hypertext TrainSfer Protocol Bost /de/cgi/login HTTP/1.1v/n Expert Info (Chat/Sequence): POST /de/cgi/login HTTP/1.1v/n] Request Wethod: POST Request VGT: /de/cgi/login HTTP/1.1v/n Expert Info (Chat/Sequence): POST /de/cgi/login HTTP/1.1v/n] Request VGT: /de/cgi/login HTTP/1.1v/n Connection: kee_0-allve/vin Connection: kee_0-allve/vin Connection: kee_0-allve/vin Content -tength: 116/ Cathe-Control: max-age=0/vin for int intry/www.gmx.atv/n user-age=0: Vin Content -tength: 116/ Cathe-Control: max-age=0/vin Accept: text/html.application/xhml;ad-0,9.*/*;q=0.8v/n Refere: http://www.gmx.atv/n Accept:-text/html.application/xhml;ad-0,9.*/*;q=0.8v/n Refere: http://www.gmx.atdp=0.7x;q=0.8v/n Accept:-text/html.application/xhml;ad-0,9.*/*;q=0.8v/n Accept:-text/html.application/xhml;ad-0,9.*/*;q=0.8v/n Accept:-text/adlevel=24/detest&dogmx.atdp=password&jsenabled=trueduinguserid=acl4087b=27496-1337244698-6 Advisered intel_dogma intervel=24.200 dogma intervel=25.100 Sol 12 C 7 3 7 4 23 24 97 33 4 7 00 97 4 4 3 29 8 5 1 24 5 0 Sol 30 C 7 30 4 0 2 6 3 3 0 0 6 0 dogma intervel Sol 30 C 7 3 5 4 3 0 3 7 6 3 3 4 3 4 3 6 3 5 9 5 1 24 5 0 Sol 30 C 7 3 7 4 5 2 3 4 2 4 3 7 7 4 7 2 5 2 4 5 3 3 4 3 0 6 7 6 4 3 5 8 5 1 2 3 5 0 Sol 5 2 7 4 5 3 3 4 3 0 6 7 6 4 3 5 8 5 1 2 3 5 0 Sol 5 2 7 4 5 3 3 4 3 0 6 7 6 4 3 5 8 5 1 2 3 5 0 Sol 5 2 7 4 5 3 3 4 3 0 6 7 6 4 5 8 5 6 6 4 3 4 7 6 5 7 7 4 5 3 4 3 4 7 9 7 7 4 7 7 6 7 5 6 6 6 6 8 7 6 5 7 6 6 7 6 7 7 6 7 7 6 7 6 6 6 8 7 6 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7</pre>		64 7.831915	140.78.100.211	217.72.203.250	HTTP	GET /?LogoutAdProxy.service=hpfirst&site=qmx§ion=qmx/homepage/start,	/at/
Line-based text data: application/x-www-form-urlencoded AREA=1&EXT=redirect&EXT2=&dlevel=c&id=test%40gmx. at&p=password&jsenabled=true&uinguserid=ac14087b-27496-1337344698-6 U250 70 74 20 43 20 49 53 47 20 95 47 20 27 37 26 64 69 72 65 23 30 7,**; q=0 3 AREA 42 74 57 74 65 76 56 24 42 74 72 75 55 6		 Hypertext Transfer Protoc POST /de/cgi/login HTTP Expert Info (Chat/set) 	col P/1.1\r\n equence): POST /de/cgi/logi	.07), Dst Port: http (; n HTTP/1.1\r\n]	80), Seq: 1	, Ack: 1, Len: 700	
0230 70 74 20 43 80 61 72 74 62 24 34 20 49 53 47 20 pt=Cnars et: 150- 0260 38 33 39 2d 31 2c 75 74 66 2d 38 37 33 9859-1,u tf=8; q=0 AR 0280 45 41 3d 30 26 66 64 66 65 66 66 66 66 66 66 66 66 66 66 66 66 66 66 67 66 6		Hypertext Transfer Protoc POST /de/cgi/login HTTP Expert Info (Chat/Se Request Method: POST Request URI: /de/cgi/ Request Version: HTTP Host: service.gmx.net\r Connection: keep-alive\ Content length: 116] Cache-Control: max-age- origin: http://www.gmx. User-Agent: Mozilla/S.C Content-Type: applicati Accept-Encoding: gzip.c Accept-Language: de-DE, Accept-Charset: ISO-885 \r\n	<pre>col p/1.1\r\n equence): POST /de/cgi/logi /login p/1.1 r\n r\n a =0r\n .at\r\n 0 (Windows NT 6.1; WOW64) A ion/x-www-form-urlencoded\r ication/xhtml+xml,applicati k.at/?status=login-failed\r 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\</pre>	07), Dst Port: http (n HTTP/1.1\r\n] n HTTP/1.1\r\n] (\n on/xm];q=0.9,*/*;q=0.1 (\n e0.4\r\n n	80), Seq: 1 ™L, like G 8\r\n	ecko) Chrome/18.0.1025.168 Safari/535.19\r\n	
0250 70 74 36 74 36 20 49 34 72 65 74 36 20 49 34 72 65 74 36 20 49 34 72 65 24 36 20 74 73 74 66 24 85 71 3d 30 2e 33 0d 0a 0d 44 52 74 <		Hypertext Transfer Protoc POST /de/cgi/login HTTP ⊕ [Expert Info (Chat/se Request Wethod: POST Request VRI: /de/cgi/ Request Version: HTTP Host: service.gmx.net\r Connection: keep-alive\ ⊖ Content-Length: 116\r\r [Content length: 116\r\r [Content length: 116\r\r [Content length: 116\r\r [Content length: 116\r\r Content-Type: applicati Accept: text/html,appli Referer: http://www.gmx Accept-Encoding: gzip,c Accept-Language: de-DE, Accept-Charset: ISO-885 \r\n ⊟ Line-based text data: app	<pre>col p/1.1\r\n equence): POST /de/cgi/logi /login p/1.1 r\n r\n 0 (Windows NT 6.1; WOW64) A ion/x-www-form-urlencoded\r ication/xhtml+xml,applicati x.at/?status=login-failed\r deflate,sdchr\n deflate,sdchr\n deflate,sdchr\n ge;q=0.8,en-US;q=0.6,en;q= 59-1,utf-8;q=0.7,*;q=0.3\r\ plication/x-www-form-urlence communication communication communication communication communication communication communication communication commu</pre>	07), Dst Port: http (pplewebKit/535.19 (KH `\n on/xm];q=0.9,*/*;q=0.3 `\n :0.4\r\n n	80), Seq: 1 TML, like G 8\r\n	ecko) Chrome/18.0.1025.168 Safari/535.19\r\n	
		 □ Hypertext Transfer Protoc □ POST /de/cgi/login HTTP □ [Expert Info (Chat/Se Request Wethod: POST Request URI: /de/cgi/ Request Version: HTTP Host: service.gmx.net\r Connection: keep-alive\ □ Content-Length: 116\r\r [Content length: 116\r\r [Content length: 116\r\r [Content length: 116\r\r Content-Type: applicati Accept: text/html,appli Referer: http://www.gmx Accept-Encoding: gzip,o Accept-Language: de-DE, Accept-Language: de-D	<pre>col p/1.1\r\n equence): POST /de/cgi/logi /login p/1.1 r\n vr\n] =0\r\n .at\r\n 0 (windows NT 6.1; WOW64) A ion/x-www-form-urlencoded\r ication/xhtml+xml,applicati x.at/?status=login-failed\r deflate,sdch\r\n deflate,sdch</pre>	07), Dst Port: http (n HTTP/1.1\r\n] hpplewebKit/535.19 (KH \n on/xm];q=0.9,*/*;q=0.3 \n 0.4\r\n n 0.4\r\n n :oded at&p=password&jsenab1	80), Seq: 1 TML, like G 8\r\n ed=true&uin	ecko) Chrome/18.0.1025.168 5afari/535.19\r\n guserid=ac14087b-27496-1337344698-6	
		 □ Hypertext Transfer Protoc □ POST /de/cgi/login HTTP □ [Expert Info (Chat/Se Request Method: POST Request Version: HTTP Host: service.gmx.net\r Connection: keep-alive\ □ Content-Length: 116\r\r [Content length: 116\r\r [Content length: 116] □ Cache-Control: max-age Origin: http://www.gmx ∪ User-Agent: Mozilla/S.O Content-Type: applicati Accept: text/html,appli Referer: http://www.gmx Accept-Charset: ISO-885 \r\n □ Line-based text data: app AREA=1&EXT=redirect&EXT 0250 70 74 26 45 58 51 22 3b 71 3d 0260 45 41 3d 31 26 45 58 0290 74 26 56 54 32 3d 0240 26 57 26 96 4 3d 0240 32 37 34 39 36 2d 31 	<pre>col p/1.1\r\n equence): POST /de/cgi/logi /login p/1.1 r\n vr\n of cation/x-www-form-urlencoded\r ication/xhtml+xml,applicati 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\ plication/x-www-form-urlenc r2=&dlevel=c&id=test%40gmx. 73</pre>	07), Dst Port: http (n HTTP/1.1\r\n] n HTTP/1.1\r\n] n HTTP/1.1\r\n] n m n m n m n m n m n m n m n m	RO), Seq: 1 TML, like G 8\r\n ed=true&uin	2cko) Chrome/18.0.1025.168 5afari/535.19\r\n 2userid=ac14087b-27496-1337344698-6	

Wireshark **HTTP authentication + TLS**

	-M				viresna
El.				H.	TTP authentication + T
	Intel(R) PRO/100 VE Network Con	nection - Wireshark			×
	<u>Eile Edit View Go Capture Anal</u>	yze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>H</u> elp			
		🗶 🛃 📇 🛛 🔍 🔅 🔹 🌍 7	<u>।</u>	0, 🖭 1	📱 🗹 幆 % 💢
	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	213.165.65.100	140.78.100.211	TLSV1	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, Applica
	27 1.834206	213.165.65.100	140.78.100.211	TLSV1	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
	28 1.892803	213.165.65.100	140.78.100.211	TLSV1	Application Data, Application Data
	39 2 016840	213 165 64 71	140 78 100 211	нттр	GET / Status=TogHT-Taffed HTP/1.1 HTTP/1 1 301 Moved Permanently (fayt/html)
	47 2.118085	140.78.100.211	213.165.64.72	НТТР	GET /2status=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	140.78.100.211	213.165.64.72	HTTP	GET /uim.html HTTP/1.1
	J 70 2.618334	140.78.100.211	217.72.204.172	нттр	GET /novar.is HTTP/1.1
		/ire, 991 bytes captured)			
	Ethernet II, Src: Intel	_40:e1:0d (00:07:e9:40:e1:0d)	, Dst: IntelCor_e9:2d	1:7f (00:13	:20:e9:2d:7f)
	Internet Protocol, Src:	213.165.65.100 (213.165.65.1	.00), Dst: 140.78.100.	211 (140.7)	8.100.211)
	⊞ Transmission Control Pro	otocol, Src Port: https (443)	, Dst Port: 12203 (12	203), Seq:	2921, Ack: 428, Len: 937
		s (3800 bytes): #22(1403), #	23(1460), #24(937)]		
	Secure Socket Laver				
	TLSv1 Record Laver: Ha	undshake Protocol: Certificat	e		
	Content Type: Handsh	nake (22)			
	Version: TIS 1.0 (0)	(0301)			
	Length: 2256	(0501)			
	Handshake Protocol:	Certificate			
	Handshake Prococor.	vetificate (11)			
	handshake type. Ce	artificate (II)			
	Length: 5232	h. 2240			
	Certificates Lengt	n: 3249			
	□ Certificates (3249	bytes)			
	Certificate Leng	jtn: 100/			
		at-commonName=service.gmx.ne	t,1d-at-organ1zat1ona	alUnitName=	GMX,1d-at-organizationName=1&1 Mail & Media GmbH,1d-at-localityName=Montabaur,1d
	Certificate Leng	jth: 1136			
	⊕ Certificate (id-	at-commonName=Thawte SSL CA,	id-at-organizationNam	ie=Thawte,	Inc.,id-at-countryName=US)
	Certificate Leng	jth: 1097			
	⊞ Certificate (id-	at-commonName=thawte Primary	' Root CA,id-at-organi	zationalUn	itName=(c) 2006 thawte, Inc For author,id-at-organizationalUnitName=Certifica
	□ TL5v1 Record Layer: Ha	andshake Protocol: Server Key	Exchange		
	Content Type: Handsh	nake (22)			
	Version: TLS 1.0 (0)	(0301)			
	Length: 525				
	🔄 🗆 Handshake Protocol:	Server Kev Exchange			
	0000 00 13 20 e9 2d 7f 00	07 e9 40 e1 0d 08 00 45 00	E.		*
	0010 03 d1 1d 6c 40 00 2d	06 24 90 d5 a5 41 64 8c 4e]@ \$Ad.N		-
	0020 64 d3 01 bb 2f ab 7e	f8 12 e0 22 f1 ac 0f 50 18	d/.~"P.		-
	0040 36 a4 77 d8 76 97 50	90 91 1T 97 6a 52 CD de 09	6 w { pp \ n) + 0+		
	0050 26 1e 09 a5 80 7h 40	2d eb e8 27 85 c9 fe 61 fd	&{@'		
	0060 7e e6 7c 97 1d d5 9d	02 03 01 00 01 a3 81 c2 30	~. 0		
	0070 81 bf 30 0f 06 03 55	1d 13 01 01 ff 04 05 30 03			
	0080 01 01 ff 30 3b 06 03	55 1d 20 04 34 30 32 30 30	0;		× I
		20 50 20 00 08 20 00 01 05			
	Frame (991 bytes) Reassembled TCP (38	DU Bytes)			
	File: "C:\Users\michael\AppData\Local\T	emp\wir Packets: 291 Displayed: 48 Marke	d: 0 Dropped: 0		Profile: Default

Serial number: Photograph



Code: NAR61HA06E040L0711214

• E1245D7N

Michael Sonntag

Serial number: According to tools

Deive Neme	Carial Number	Devision	Attacked	-			
E040L0	ABCDEF0000125EF7	NAR6	Yes				
				Мах	ctor 6 E040L0 USB De	vice Properties	
				G	eneral Policies Volum	nes Driver Details	
Help-About	New Firmware	Check	Close	c	Maxtor 6 E040	LO USB Device	
http://support seagate.com/firmware/drive.config.html			Device type:	Disk drives			
http://support.seagate.com/htmware/drive_coning.htm				Manufacturer:	(Standard disk drives)		
					Location:	on USB Mass Storage Device	
				ſ	Device status		
					This device is working	ı properly.	

Cancel

OK

Michael Sonntag

FU

Serial number: X-Ways Forensic

echnical 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	-	
<u>C</u> opy All Close	Help	

Serial number: Web information



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

Maxtor DiamondMax Plus 8 Made under U.S. and foreign patents issued and pending. Maxtor is not responsible for consequential damages, including loss or recovery of data. For full warranty, patent and installation information, contact: www.maxtor.com DiamondMax Plus 8 40GB ATA/133 HDD Date: 23AUG2002 +12V 790mA +5V 647mA Code: FWFWFWFW LBA: 195313104 ER: XXXXXXX 3.5 SERIES CN256 E-H011-01-0101 6E040L0110101 Model Number SN: E100001F (First 7 characters) H,D,M,P Serial Number

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

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
 - \rightarrow Ca. 850 MB/min

Ele Edit Help Status 3% Input Size 38.287GB Input: \Device\Harddisk7 (entire disk) Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/s
Status 3% Input Size 38.287GB Input: \Device\Harddisk7 (entire disk) Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/s
3% Input Size 38.287GB Input: \Device\Harddisk7 (entire disk) Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/s
Input Size 38.287GB Input: \Device\Harddisk7 (entire disk) Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/S
Input: \Device\Harddisk7 (entire disk) Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/s
Output: C:\Data\tmp\disk.img.gz Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/S
Bytes read: 1.262GB Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/S
Skipped: N/A Bytes written: 575.511MB Current speed: 9.916MB/s
Bytes written: 575.511MB Current speed: 9.916MB/s
Current speed: 9.916MB/s
Average speed: 8.304MB/s
Start Cancel

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

Questions?

Thank you for your attention!

F

Literature/Links

- 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/