# Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise

Bindu Dodiya Institute of computer Science Vikram University Ujjain

### ABSTRACT

Packet analysis is a primary trace back technique in network forensics, Packet analysis, often referred to as packet sniffing or protocol analysis, describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network. This can be used to find traces of nefarious online behavior, data breaches, unauthorized website access, malware infection, and intrusion attempts, and to reconstruct image files, documents, email attachments, etc. sent over the network .Packet analysis is typically performed using a packet sniffer, a tool used to capture raw network data going across the wire. Wireshark proves to be an effective open source tool in the study of network packets and their behavior. In this regard, Wireshark can be used in identifying and categorizing various types of attack signatures. It lets administrator to see what's happening on network at a microscopic level. The purpose of this paper is to demonstrate how Wireshark is applied in network protocol diagnosis and can be used to find some basic indicators of compromise for a malware.

#### **Keywords**

Packet analyis, Indicators of compromise IOC, wireshark, Maware

### 1. INTRODUCTION

In today's world, computer networks have become smarter and much more complex. At the same time, hackers across the world are designing and inflicting various types of attacks through the internet for different reasons such as information theft, machine corruption and hijacking. These attacks affect most system users including the administrators and forensic investigators [1]. All these issues impel network engineers to be able to analyze network traffic and understand its behavior. As the number Organizations must regularly check their resources for the presence of malicious components. One of the ways in which a resource may become infected is as a result of vulnerability exploitation by cybercriminals. At the time of exploitation, experts may investigate incidents related to the threat. Moreover, some findings of these investigations may already be publicly available. Such reports have practical value. A typical report on an Advanced Persistent Threat (APT) campaign also includes Indicators of compromise .By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent them or limit damages by stopping attacks in earlier stages. Of all the detailed technical information on any given Advanced Persistent Threat (APT), "indicators of compromise" have the greatest practical value for security administrators [2].Indicators of compromise aid information security and IT professionals in detecting data

Umesh Kumar Singh, PhD Institute of Computer Science Vikram University Ujjain

breaches, malware infections, or other threat activity. When a host is infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic to identify affected hosts and users. Captured packets can reveal the signatures of attacks, and this information can enable the users to recover the systems from damages caused by the attackers.

There are two aspects that make packet analysis very important. First, packet analysis is part of the baselines of anything important to a network because it allows knowing the state of a network in advance before problems arises [3]. Second, packet analysis is useful to diagnose a network in the case of attack, and it helps network administrators look into wires and know the traffic traversing them or the issues that might be present[4]. The later aspect is the foundation of network forensics with packet analysis tools like Wireshark. Analyzing packets with the goal of enforcing network security can help network users with the following [5]:

- Understanding network characteristics Learning who is
   on a network
- Determining who or what is utilizing available bandwidth
- Identifying peak network usage times
- Identifying possible attacks or malicious activity
- Finding unsecured and bloated applications

In this paper it has been described that how packet analysis tool like wireshark can be used to collect values for some basic indicators of compromise. The second section describes features and benefits of wireshark. The third section describes process of collecting basic indicators of compromise with example followed by discussion and conclusion.

## 2. PACKET SNIFFING USING WIRESHARK

There are various types of packet-sniffing programs, including both free and commercial ones. Each program is designed with different goals in mind. A few popular packet-analysis programs are tcpdump, OmniPeek, and Wireshark .tcpdump is a command-line program. OmniPeek and wireshark. Wireshark have graphical user inter-faces (GUIs).**Wireshark** is the world's foremost and widely-used network protocol analyzer. It lets us see what's happening in our network at a microscopic level. [6] .Wireshark offers several benefits that make it appealing for everyday use. It is aimed at both the journeyman and the expert packet analyst, and offers a variety of features to entice each.

### 2.1 Benefits of Wireshark

- **Supported protocols :** Wireshark supports more than 850 protocols. These range from common protocols like IP and DHCP to more advanced proprietary protocols like AppleTalk and BitTorrent. Wireshark is developed under an open source model, new protocol support is added with each update.
- User-friendliness : The Wireshark interface is one of the easiest to understand of any packetsniffing application. It is GUI-based, with very clear context menus and a straightforward layout. Wireshark provides several features designed to enhance usability, such as protocolbased color coding and detailed graphical representations of raw data. command line interface of other packet sniffing tool like tcpdump is very complicated while The Wireshark GUI is great for those who are just entering the world of packet analysis.
- **Cost**: Wire- shark is released as free software under the GPL. it can be downloaded from it's official website and can be used for personal or commercial purpose.
- **Program support :** The Wireshark web page have links which directs to several forms of support, including online documentation, a support and development wiki, FAQs, and a place to sign up for the Wireshark mailing list, which is monitored by most of the program's top developers. Paid support for Wireshark is also available from CACE Technologies through its SharkNet program.
- **Operating system support :** Wireshark supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms. complete list of supported operating systems is available on the Wire- shark home page.

### 2.2 Collection of IOCs using wireshark

Indicators of compromise (IOCs) are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in earlier stages[1] Monitoring for indicators of compromise enables organizations to better detect and respond to security compromises. Collecting and correlating IOCs in real time means that organizations can more quickly identify security incidents that may have gone undetected by other tools and provides the necessary resources to perform forensic analysis of incidents. If security teams discover recurrence or patterns of specific IOCs they can update their security tools and policies to protect against future attacks as well .Wireshark is a popular tool for troubleshooting network related issues. When a host is

infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic . and these packet captures can be used to identify affected hosts and users. Collection of IOCs help organizations to detect and prevent attack. In this section it is explained that how to Collect following IOC for malware using wireshark.

- File Hashes
- Host IP address
- Domain Name
- Host Name
- MAC address of host

Wireshark can be used in two ways one is to perform local capture and other is to analyze packet captures already available .There are many sites that provide pcap for analysis .we have used pcap from Traffic analysis exercise Pizza Bender. [7]

### (I) Finding the Hash of infected file

The fundamental goal of web analytics is to collect and analyze data related to web traffic and usage patterns. The data mainly comes from four sources[8]

- Direct HTTP request data: directly comes from HTTP request messages (HTTP request headers).
- Network level and server generated data associated with HTTP requests: not part of an HTTP request, but it is required for successful request transmissions for example, IP address of a requester.
- Application level data sent with HTTP requests: generated and processed by application level programs (such as JavaScript, PHP, and ASP.Net), including session and referrals. These are usually captured by internal logs rather than public web analytics services.
- External data: can be combined with on-site data to help augment the website behavior data described above and interpret web usage. For example, IP addresses are usually associated with Geographic regions and internet service providers, e-mail open and click-through rates, direct mail campaign data, sales and lead history, or other data types as needed.For Collecting hash of infected file follwing steps has been followed
  - (i) apply filter http.request in wireshark .
  - (ii) from the resuts of step(i) get the affected files from http objects.
  - (iii) Save the affected file(.in this example found file is a php file).
  - (iv) Get Hash of the file saved .

In this example Obtained Hash of infected file using wireshark is : a52a1e151bf4b993efcff87b3780d731 Screenshot of above process is presented in fig1.

2020-08-21-traffic-analysis-exercise.pcap			-				- 0 X	k
File Edit View Go Capture Analyze Statis	stics Telephony Wireless	Tools Help						
📕 🗏 🛞 🔰 🛅 🕱 🗳 🔶 🕾	7 1	<b>L</b>						
http.request							X 🖘 🔹	+
No. Time src por	t Source	dst port	Destination	Protocol	Length Host	Info		
8 2020-08-21 20:33:06.624945 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
11 2020-08-21 20:33:06.923092 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
70 2020-08-21 20:33:07.908598 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
150 2020-08-21 20:33:09.640765 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	100
208 2020-08-21 20:33:10.908359 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
216 2020-08-21 20:33:13.908271 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
692 2020-08-21 20:34:24.612762 612	208 10.8.21.163	80	45.12.4.190	HTTP	318 ncznw6a.com	GET /dujok/kevyl.p	hp?l=ranec11.cab HTTP/1.1	
5418 2020-08-21 20:41:02.619751 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
5419 2020-08-21 20:41:05.621284 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	
5444 2020-08-21 20:41:08.636931 545	511 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.2	50:1900 M-SEARCH * HTTP/1.	1	+
Simple Service Discovery Protocol           0         Simple Service Discovery Protocol           0         Simple Service Discovery Protocol	1184 ncznw6a.com	application/octet-stre	am 304 kB kevyl.php?l=ra	inec11.cab				
0010 00 a5 27 f5 00 00 04 11 7e ae 0a 0	08							
0010         ff fa d4 ef 07 6c 00 91         20 ad d4           0030         43 46 2c 2a 20 48 54 54 50 62 ff 31           0040         64 78 2c 2a 20 48 54 54 50 62 ff 31           0040         6f 73 74 3a 20 32 33 39         2e 32 35           0050         24 22 35 30 3a 31 39 30         30 6d 68           0060         72 67 3a 64 65 76 69 63 65 3a         66 56 64 61 73 2d           0080         6f 72 67 3a 64 65 76 69 63 65 3a         3a 31 6d 8a 4d 61 66 37 a 2d 22 73           0080         66 75 76 36 36 76 67 75 72 22 d6 48 4d         68 67 75 72 22 2d 8a 4d 8a 4d	2d Text Filter: 25 35 35 35 35 35 35 35 36 46 57 46 57 46 57 46 57 46 57 46 57 46 57 46 57 57 46 57 57 57 57 57 57 57 57 57 57	Save em as-upnp- vi ce:Inter ew ayDevice n: "ssdp:d r"MX: 3.	Save All Close	He				
0050 0a 0d 0a		•• •• •• •• •• •• •• •• •• •• •• ••			II.	Packets: 7894 · Displayed: 14 (0.7%)	Profile: Defz	ault
- Request bolican				_	11.1		Folle: Deta	sat
🔗 (C) 📄 🍳 🧿	1 🛷 🖺 👔		and the second				▲ 🍢 🛱 .all ⊕) 5:21 PM 9/2/2020	

Fig 1 finding hash of an infected file using wireshark

### (Ia) Checking whether the file is infected or Not:

By applying filter http.request a file and its hash can be found in(I). In next step it has to be checked whether the file is malicious or not .For this obtained file hashes has been checked at virustotal.com. VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004. VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.Files up to 650 MB can be uploaded to the website, or sent via email (max. 32MB). Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and, by extension, VirusTotal's own capability. Suspected URL's can be scanned and search through the VirusTotal dataset. VirusTotal for dynamic analysis of malware uses the Cuckoo sandbox.[9].

After scanning obtained file hashes on virustotal it has been found that file hashes are infected results are depicted in fig2.

💋 Using   M (no sut   🕲 I	ror 4 🛛 🚍 EN - Pr 🗍 🚱 Reser	Micros A Chapte	Wiresh   e! Post G	What a Malwa	🛛 📶 8.4. Th	W Web a 🚺 Vir 🗙	+
---------------------------	-----------------------------	-----------------	--------------------	--------------	-------------	-----------------	---

054ff4620aaa40928ca	67a2c364bedf71d79672874d75ba50ff8231069ad74d9		Q 🛧 🎬 🖵 Sign in	Sign up			
35	1 35 engines detected this file		C				
Community Score	054ff4620aaa40928ca67a2c364bedf71d79672874d75ba50ff8231069ad7 hote.dll pedli	4d9	297.50 KB 2020-08-26 05:15:17 UTC Size 7 days ago				
DETECTION DET	TAILS RELATIONS BEHAVIOR COMMUNITY						
Ad-Aware	① Gen:Variant.Zusy.311755	AegisLab	Trojan.Win32.Zusy.4lc				
Alibaba	Trojan:Win32/IcedId.fc160525	ALYac	Trojan.lcediD.gen				
SecureAge APEX	Malicious	Arcabit	Trojan.Zusy.D4C1CB				
AVG	() Win32:Malware-gen	Avira (no cloud)	TR/AD.PhotoDider.DD				
BitDefender	() Gen:Variant.Zusy.311755	BitDefenderTheta	() Gen:NN.ZedlaF.34196.su8@aW4giTbi				
Comodo	() .UnclassifiedMalware@0	Cyren	U W32/Trojan.OESC-3018				
DrWeb	() Trojan.lcedID.30	Elastic	() Malicious (high Confidence)				

Fig2.Sacnning results on virustotal.com

### (II) Finding the host name, Domain name, IP address and MAC address:

Any host generating traffic within the network should have three identifiers: a MAC address, an IP address, and a hostname. In most cases, alerts for suspicious activity are based on IP addresses.[10] If the access is avaiable to full packet capture of the network traffic, a pcap retrieved on an internal IP address should reveal an associated MAC address and hostname. Host information can be found using Wireshark by applying filter on two types of activities: Dynamic Configuration Host Protocol (DHCP) or NetBIOS Name Service (NBNS). DHCP traffic can help identify hosts for almost any type of computer connected to the network. DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network [11]. NBNS traffic is generated primarily by computers running Microsoft Windows or Apple hosts running MacOS.. Depending on how frequently a DHCP lease is renewed, DHCP traffic might not be there in pcap. Fortunately,in this case NBNS traffic can be used to identify hostnames

for computers running Microsoft Windows or Apple hosts running MacOS .

In experiment presented in this paper host details have been found from NBNS traffic steps for obtaining host name, domain name,IP address and MAC address are as follows

- (i) apply nbns as filter as depicted in fig3
- (ii) for given source IP obtained the host DESKTOP-OF4FE8A<20> and
- (iii) Domain Name can be found under hyper text transfer protocol in second window of wireshark as depicted in fig4 .
- (iv) Obtained Domain is ncznw6a.com.
- (v) Ger IP address of the host under Internet protocol in same window
- (vi) Obtained IP addrees of host is 10.8.21.163.
- (vii) IP address of infected machine is 45.12.4.190
- (viii) MAC address of infected machine is 10:c3:7b:0a:f2:85 as depicted in fig5.

File Edit View Go Capture Analyze	Statistics Telephony W	ireless Tools Help					
📕 🗏 🛞 📕 🖾 🗙 🖾 🍳 👄 👄	🕾 T 🛓 📃 🔍 🔍	ର୍ ର୍ 🎹					
nbns							+ ~ 🖾
No. Time sr	c port Source	dst port	Destination	Protocol	Length Host	Info	*
1 2020-08-21 20:33:06.470838	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
2 2020-08-21 20:33:06.471055	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<00>	
3 2020-08-21 20:33:06.471294	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	
14 2020-08-21 20:33:07.250402	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	E
15 2020-08-21 20:33:07.250621	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<00>	
16 2020-08-21 20:33:07.250909	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
83 2020-08-21 20:33:08.001018	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
84 2020-08-21 20:33:08.001194	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<00>	
85 2020-08-21 20:33:08.001304	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	
121 2020-08-21 20:33:08.751244	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	
122 2020-08-21 20:33:08.751462	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<00>	and a second
123 2020-08-21 20:33:08.751605	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
3596 2020-08-21 20:38:11.892364	137 10.8.21.163	137	10.8.21.255	NBNS	92	Name query NB PIZZA-BENDER<1b>	
3597 2020-08-21 20:38:11.892542	137 10.8.21.8	137	10.8.21.163	NBNS	104	Name query response NB 10.8.21.8	
<ul> <li>Source: ASUSTekc_0a:f2:85 (10:c2 Type: IPv4 (0x0800)</li> <li>Internet Protocol Version 4, Src: 1 0100 = Version: 4  0101 = Header Length: 20 by</li> </ul>	8:7b:0a:f2:85) 10.8.21.163, Dst: 10.8 rtes (5)	8.21.255					-
0000 ff ff ff ff ff ff 10 c3 7b 0a	f2 85 08 00 45 00	·····E·					
0010 00 60 05 ea 00 00 80 11 f4 f1	0a 08 15 a3 0a 08	Contraction of the second s					
0020 15 TT 00 89 00 89 00 4C DC 90	46 46 44 45 4c 46	E FEFEDELE					
0040 45 45 50 46 41 43 4e 45 50 45	47 44 45 45 47 45	EPEACNE PEGDEEGE					
0050 46 44 49 45 42 43 41 00 00 20	00 01 c0 0c 00 20 F	DIEBCA-					
0060 00 01 <u>00 04 93 e0</u> 00 05 00 00	0a 06 15 a3						
😑 🍸 Source Hardware Address (eth.src), 6 byte	25					Packets: 7894 · Displayed: 20 (0.3%)	Profile: Default
📀 🥝 📋 🛛 🚺	🌍 🖬 🖉		-			- N 0 at 0	5:38 PM 9/3/2020

Fig3.Finding hostname from NBNS traffic using wireshark

2020	0-08-21-traffic-analysis-exerc	tise.pcap	and a second	States in the low			Sec. Sec.	A free way the	
File	Edit View Go Capture	Analyze	Statistics Telephony V	/ireless Tools Help					
		<b>q</b> @ #	>≌ ? ⊻[_] = °						
ncp	request			12		<b>D</b> 1 1	a second		
NO.	Time	4 610760	src port Source	dst port	Destination	Protocol	Length Host	INTO	23 annual ach UTTD/A A
1 1	092 2020-00-21 20:04:2	4.012/02	01200 10.0.21.103 80 45 12 4 100	61208	45.12.4.190	HITP	S16 ncznwoa.com	UEI /dujok/kevy1.php	ri=ranecii.cab miiP/1.i
+ 1	104 2020-08-21 20:54:2	0.746242	60 45.12.4.190	01208	10.0.21.103	HTTP	814 241 et 1d1 ut edeueue	HITP/1.1 200 OK	
6	+07 2020-00-21 21:25:0	2.733400	012/0 10.0.21.105	61379	10 0 11 162	HITP	201	HTTP/1 1 204 Not More	ified
6	10 2020-00-21 21.23.0	2 852010	61278 10 8 21 163	80	8 252 146 254	HTTP	336 ctldl windowsun	data com GET /msdownload/unda	te/w3/static/trustedr/en/nincul
6	12 2020-08-21 21.23.0	2.032019	80 8 252 146 254	61278	10 8 21 163	HTTP	380	HTTP/1 1 304 Not Mor	ified
74	136 2020-08-21 22:23:0	3 992139	61315 10 8 21 163	80	205 185 216 10	HTTP	341 ctldl windowsun	date com GET /msdownload/unda	te/v3/static/trustedr/en/disall
74	138 2020-08-21 22:23:0	4.092685	80 205 185 216 1	61315	10.8.21.163	HTTP	244	HTTP/1.1 304 Not Mor	ified
74	139 2020-08-21 22:23:0	4.103630	61315 10 8 21 163	80	205, 185, 216, 10	HTTP	336 ctldl.windowsun	date com GET /msdownload/unda	te/v3/static/trustedr/en/ninrul
74	141 2020-08-21 22:23:0	4 182750	80 205 185 216 10	61315	10 8 21 163	HTTP	245	HTTP/1 1 304 Not Mod	ified
	Accept-Language: en-US Accept-Encoding: gzip, User-Agent: Mozilla/4.	5\r\n deflate 0 (compa	\r\n tible; MSIE 7.0; Windo	ws NT 10.0; WOW64; <sup>-</sup>	Trident/7.0; .NET4.0C;	.NET4.0E)\r	\n		
	Host: ncznw6a.com\r\n								
0060	31 0d 0a 41 63 63 65	70 74 3	a 20 2a 2f 2a 0d 0a	1Accep t: */*					
0070	41 63 63 65 70 74 2d	4c 61 6	e 67 75 61 67 65 3a	Accept-L anguage:					
0000	20 05 06 20 55 55 00 6e 63 6f 64 69 6e 67	23 20 6	7 7 69 79 76 76 64	en-US·· Accept-E					
00a0	65 66 6c 61 74 65 Ød	0a 55 7	3 65 72 2d 41 67 65	eflate. User-Age					
0ebe	6e 74 3a 20 4d 6f 7a	69 6c 6	c 61 2f 34 2e 30 20	nt: Mozi lla/4.0					_
00c0	28 63 6f 6d 70 61 74	69 62 6	c 65 3b 20 4d 53 49	(compati ble; MSI					
00d0	45 20 37 2e 30 3b 20	57 69 6	e 64 6f 77 73 20 4e	E 7.0; W indows N					
00e0	54 20 31 30 2e 30 3b	20 57 4	f 57 36 34 3b 20 54	T 10.0; WOW64; T					-
0100	72 69 64 65 66 74 2T	3/ 2e 3	0 3D 20 2e 4e 45 54	A OC: N ETA OE).					
0110	0a 48 6f 73 74 3a 20	4e 45 54	+ 54 28 50 45 29 00 - 68 77 36 61 28 63	Host: n cznw6a c					
0120	6f 6d 0d 0a 43 6f 6e	6e 65 63	3 74 69 6f 6e 3a 20	Conn ection:					
0130	4b 65 65 70 2d 41 6c	69 76 65	5 0d 0a 0d 0a	Keep-Ali ve····					•
0 7	HTTP Host (http.host), 19 b	ytes					Pa	ckets: 7894 · Displayed: 10 (0.1%)	Profile: Defaul
-	e a	0	O 🧭 🛯						▲ 🎼 👘 .all �) 5:51 PM 9/2/2020

### Fig 4 finding domain address using wireshark

1	2020-08-2	-traffic-ar	alysis-exer	cise.pcap		-	-	10					- 0 -×	
Fil	le Edit	/iew Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools Hel	lp					
4	<b>I</b> <i>d</i> :	a 🔒 🛛	5 🗙 🗃	9 00 0	a es a	ADE	) e e e	R.R						
	http://www.	e i e c				× (2) (=		- abda						+
	nupreque	201			0.000			1.1	5 . F. F		la carta de la			
NO		ne		C C24045	src port	Source		ast port	Destination	Protocol	Length Host			ĥ
	11 2	20-00-2	1 20:55:0	0.024945	54511	10.0.21.10	2	1000	239.235.255.25	0 550P	179 239.255.255.250.1900	M-SEARCH # HTTD/1.1		
	70.0	20-00-2	1 20:55:0	7 000500	54511	10.0.21.10		1000	239.235.255.25	0 550P	179 239.255.255.250.1900	M CEADCH & UTTD/1.1		
	150 2	20-00-2	1 20:55:0	0 640765	54511	10.0.21.10	2	1000	209.200.200.20	0 SSUP	179 239.235.255.250.1900	M SEARCH # HTTD/1 1		
	208 2	20-00-2	1 20.33.0	0 008350	54511	10.8.21.16	2	1000	233.233.233.23		179 239.255.255.256.1900	M_SEARCH # HTTD/1 1		
	200 2	20-00-2	1 20.33.1	3 008271	54511	10.8.21.10	2	1000	239.255.255.25		179 239 255 255 250 1000	M_SEADCH * HTTD/1 1		
-I.	692 2	20-08-2	1 20.34.3	4 612762	61208	10 8 21 16	,	80	45 12 4 190	HTTP	318 pczpw6a com	GET /dujok/keyv] nhn?]=canec11 cab HTTP	0/1 1	E
- Ke	5418 2	20-08-2	1 20.41.0	619751	54511	10 8 21 16		1900	239 255 255 25		179 239 255 255 250 1988	M-SEARCH * HTTP/1 1	/ - 1 -	
	5419 2	20-08-2	1 20:41.0	5.621284	54511	10.8.21.16	3	1900	239 255 255 25	0 SSDP	179 239 255 255 250 1900	M-SEARCH * HTTP/1.1		
	5444 2	20-08-2	1 20.41.0	8 636931	54511	10 8 21 16	1	1900	239 255 255 25	e SSDP	179 239 255 255 250 1900	M-SEARCH * HTTP/1 1		
	6407 2	20-08-2	1 21:23:0	2.735468	61278	10.8.21.16	1	80	8,252,146,254	HTTP	341 ctldl.windowsundate.co	om GET /msdownload/undate/v3/static/truste	dr/en	
	6410 2	20-08-2	1 21:23:6	2.852019	61278	10.8.21.16		80	8,252,146,254	HTTP	336 ctldl.windowsupdate.co	om GET /msdownload/update/v3/static/truste	dr/en	
	7436 2	20-08-2	1 22:23:0	3.992139	61315	10.8.21.16	3	80	205,185,216,10	HTTP	341 ctldl.windowsupdate.co	om GET /msdownload/update/v3/static/truste	dr/en	
	7439 2	20-08-2	1 22:23:0	4.103630	61315	10.8.21.16	3	80	205.185.216.10	HTTP	336 ctldl.windowsupdate.co	om GET /msdownload/update/v3/static/truste	edr/en	+
-	Time	ka 14	128				-11	2000.0						
	Proto	col: TCP	120											2
	Heade	c checks	(0)	Aa [valid	lation di	cabled								-
	THead	er check	cum ctat	us: Unver	ified]	Sabiea								-
	Source	<ul> <li>10.8</li> </ul>	21 163	us. onver	Intedj									
	Desti	nation:	45.12.4.	190										2
2	Transmis	sion Cor	trol Pro	tocol. Sr	c Port:	61208, Dst	Port: 80.	Sea: 1. A	lck: 1. Len: 264					
	The second second	-												*
00	010 01 3	8c 09	40 00 80	06 1c 4	a 0a 08	15 a3 2d 0c	· · · · @ · ·	• • 3 • • • •	•					*
06	120 04 b	e et 18	00 50 15	50 87 8	d al /d	0d 54 50 18		T /dutel	le le					-
00	100 11 1	65 76	70 6c 2a	70 68 7	0 21 04	3d 72 61 66	/kewl	hn?l=rai	r.					
00	150 65 6	3 31 31	2e 63 61	62 20 4	8 54 54	50 2f 31 2e	ec11.ca	HTTP/1						
06	60 31 0	d 0a 41	63 63 65	70 74 3	a 20 2a	2f 2a 0d 0a	1 · · Acce	t: */*.						11
00	070 41 6	63 65	70 74 2d	4c 61 6	ie 67 75	61 67 65 3a	Accept-	anguage	:					
00	80 20 6	5 6e 2d	55 53 Ød	0a 41 6	3 63 65	70 74 2d 45	en-US	Accept-	E					
00	90 6e 6	3 6f 64	69 6e 67	3a 20 6	7 7a 69	70 2c 20 64	ncoding	gzip,	d					
00	0a0 65 6	6 6C 61	74 65 Ød	0a 55 7	3 65 72	2d 41 67 65	eflate	User-Age	e					
00	000 be /	+ 3a 20	40 6T /a	69 60 6	C 61 2T	34 2e 30 20	nt: Moz	blor MS	T					
00	3de 45 2	37 2e	30 3b 20	57 69 6	e 64 6f	77 73 20 40	F 7.0:	indows I	N					
06	e0 54 2	31 30	2e 30 3b	20 57 4	f 57 36	34 3b 20 54	T 10.0;	WOW64;	T					÷
C	🔰 🛛 Sou	rce (ip.src)	, 4 bytes	nother start s				10212013(-15)	.M		Packets: 78	94 · Displayed: 14 (0.2%)	Profile: Defa	ault
1			-	-	~	_0.	aure l						5-11 PM	
	7 (	e		0	9							- 🗟 🛛 all 4	9/3/2020	

#### Fig5 finding IP address of infected Host

### **3. DISCUSSION**

In section 3 procedure for finding answer for following questions using Wireshark has been explained

- 1. What are the infected file downloaded and their Hashes?
- 2. What is URL Domain of infected site?

- 3. What is the IP address of infected Machine?
- 4. What is the Host Name of infected Machine?
- 5. What is the MAC address of infected Machine?

The first part infected file hashes can be blocked inside network using virus guard .Access to the infected sites and their addresses can be blocked. Investigation on infected PC whose MAC address can be made. infected files can be cleaned. In this way wireshark can be used to protect System.

Millions of new virus signatures are released yearly, and an antivirus can only detect viruses for known valid signatures and the unknown signatures escape the detection. today's networks are facing threats more than virus, such as malware, denial of service, port scanning covert channels, and information theft.however, antivirus software can only take very limited action on these various threats. Hackers can also target the antivirus software running on a machine, leading to multiple vulnerabilities of the system without the awareness of the user. For these different reasons, network traffic analysis at the packet level is necessary, and it can identify many different threats and attacks that could remain unnoticed by antivirus software. In the past, packet analyzers were very expensive and patented. Wireshark has changed all that. Wireshark is one of the best open source packet analysers available today, and it displays packet data as detailed as possible.

### **4**.CONCLUSION

The cases of packet analysis demonstrated in this paper by collecting values for Indicators of compromise will help to realize packet analysers, especially WireShark which is crucial to network forensics. "Indicators of compromise" helps to use threat data effectively, identify malware and quickly respond to incidents. Packet analyzer like wireshark can be used for security. However, despite its rich toolset, it is important to keep in mind that Wireshark is not an intrusion detection system. WireShark will not warn us when someone does strange things on network that he is not allowed to do, and it will not manipulate things on the network such as sending packets. The usefulness of Packet analyzer is that it is a convenient and effective tool that can help network security professionals figure out what is really happening in the network if strange things happen. As it has demonstrated in the paper, packet analysis in WireShark can discover a broad range of security threats and attacks against networked Computer systems.

### **5. REFERENCES**

[1] Takahashi, D., Xiao, Y. and Meng, K. (2011) 'Virtual flow-net for accountability and forensics of computer

and network systems', (Wiley Journal of) Security and Communication Networks, Vol. 7, No. 12, December, pp.2509–2526.

- [2] Denis Makrushin" Indicators of Compromise as an Instrument for Threat Intelligence "Research article available online at https://www.researchgate.net/publication/349211330, Published in august 2015.
- [3] Thor, J. (2009) Why You Need a Network Analyzer, online available http://www.technewsworld.com/story/67411.html
- [4] Meng, K., Xiao, Y. and Vrbsky, "Building a wireless capturing tool for WiF", Wiley Journal of Security and Communication Networks, Vol. 2, No. 6, November–December S.V. (2009), pp.654–668.
- [5] Vivens Ndatinya, Zhifeng Xiao, Vasudeva Rao Manepalli, Ke Meng and Yang Xiao "Network forensics analysis using Wireshark" Article in International Journal of Security and Networks · Vol. 10, No. 2, 2015.
- [6] Chris Sanders "Practical Packet Analysis Using Wireshark to solve Real-World Network Problems" 2<sup>nd</sup> Edition
- [7] https://www.malware-traffic-analysis.net/trainingexercises.html 2020-08-21 -- Traffic analysis exercise
   - Pizza-Bender.
- [8] Jack G Zheng, Svetlana Peltsverger "Web Analytics Overview" In book: Encyclopedia of Information Science and Technology, Third Edition Chapter: 756 Publisher: IGI Global January 2015
- [9] https://en.wikipedia.org/wiki/VirusTotal.
- [10] Richard Sharpe, Ed Warnicke, Ulf Lamping" Wireshark User's Guide Version" 3.7.0 available online at https://www.wireshark.org/docs/wsug html/.
- [11] Allied Telesis "Dynamic Host Configuration Protocol - DHCP Feature Overview and ConfigurationGuide"availableonlineathttps://www.all iedtelesis.com/sites/default/files/documents/configura tion-guides/dhcp\_feature\_overview\_guide.pdf