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.

			T 1 111				
		tics Telephony Wirel					
	९ ⇔ ⇒ ≌	1 🕹 📃 🗐 🍳 🤆	α ⊂ι ₩				
http.request							X 📑 🗙
o. Time	src port	Source	dst port	Destination	Protocol	Length Host	Info
8 2020-08-21 20:33:	06.624945 545	11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
11 2020-08-21 20:33:	06.923092 545	11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
70 2020-08-21 20:33:		11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
150 2020-08-21 20:33:		11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
208 2020-08-21 20:33:	10.908359 545	11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
216 2020-08-21 20:33:	13.908271 545	11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
692 2020-08-21 20:34:		08 10.8.21.163	80	45.12.4.190	HTTP	318 ncznw6a.com	GET /dujok/kevyl.php?l=ranec11.cab HTTP/1.1
5418 2020-08-21 20:41:		11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
5419 2020-08-21 20:41:		11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
5444 2020-08-21 20:41:	08.636931 545	11 10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
010 00 a5 27 f5 00 00 0	411 7eae0a0	8 Tauk Elhan				_	
010 00 a5 27 f5 00 00 0 020 ff fa d4 ef 07 6c 0	411 7eae0a0 991 20ad4d2	d Text Filter:					
00 a5 27 f5 00 00 04 020 ff fa d4 ef 07 6c 04 030 43 48 20 2a 20 48 54	4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2	d Text Filter:	Save	Save Ali Close	e He	ep	
00 a5 27 f5 00 00 00 00 ff fa d4 ef 07 6c 00 00 43 48 20 2a 20 48 50 040 6f 73 74 3a 20 32 32	4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2 3 39 2e 32 35 3	78 Text Filter:	Save	Save All Close	e He	ep	
00 a5 27 f5 00 00 6 020 ff fa d4 ef 07 6c 0 0300 43 48 20 22 48 5 040 6f 73 74 3a 20 32 3 050 22 32 35 30 3a 13 3 050 72 6e 3a 73 36 68 66	4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2 3 39 2e 32 35 3 9 30 30 0d 0a 5 5 6d 61 73 2d 7	18 de 5 3 5 70 6e 70 2d rn:	schem as-upnp-	Save All Close	e He	ep	
010 00 a5 27 f5 00 00 0 020 ff fa d4 ef 07 6c 0 030 43 48 20 2a 24 85 2 040 6f 73 74 3a 20 32 3 050 2e 32 35 30 3a 13 3 050 7e 3a 7a 3a 63 68 6 070 6f 72 67 3a 64 65 7	4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2 3 39 2e 32 35 3 9 30 30 0d 0a 5 55 6d 61 73 2d 7 6 69 63 65 3a 4	R d e 5 3 5 70 6e 70 2d rn: 9 6e 74 65 72 org	schem as-upnp- :devi ce:Inter	Save Al Close	e He	ep	
00 a5 27 f5 00 00 a 120 ff fa d4 ef 07 c6 0 304 43 48 20 2a 2a 43 32 34 3040 67 73 3a 20 48 52 32 35 3a 3a </td <td>4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2 3 39 2e 32 35 3 9 30 30 0d 5 5 6d 61 73 2d 7 5 69 63 65 3a 4 5 77 61 79 44 6</td> <td>Text Filter: 5 70 6e 70 2d rn: 9 6e 74 65 72 org 9 6e 74 65 72 org 5 76 69 63 65 net</td> <td>schem as-upnp- :devi ce:Inter Gatew ayDevice</td> <td>Save Al Cose</td> <td>e He</td> <td>•</td> <td></td>	4 11 7e ae 0a 0 0 91 20 ad 4d 2 4 54 50 2f 31 2 3 39 2e 32 35 3 9 30 30 0d 5 5 6d 61 73 2d 7 5 69 63 65 3a 4 5 77 61 79 44 6	Text Filter: 5 70 6e 70 2d rn: 9 6e 74 65 72 org 9 6e 74 65 72 org 5 76 69 63 65 net	schem as-upnp- :devi ce:Inter Gatew ayDevice	Save Al Cose	e He	•	
00 a5 27 f5 00 00 0 200 df fa d4 ef 07 06 0	4 11 7e ae 0a 0 0 0 ad 4d 2 ad 4d 2 ad 4d 2 ad 3d 2 ad 3d 2 ad 3d 2 ad 3d ad ad	8 Text Filter: 9 5 70 6e 70 2d rn: 9 6e 74 65 72 org 5 76 69 63 65 net 3 64 70 3a 64 :1	schem as-upnp- :devi ce:Inter Gatew ayDevice ·Man: "ssdp:d	Save Al Close	e He	eip	
110 00 a5 27 f5 00 00 a5 0200 ff fa d4 ef 07 6c 00 0201 ff fa d4 ef 07 6c 00 0203 ff fa d4 ef 07 6c 00 0203 ff fa d4 20 2a 20 43 32 0203 ff fa d2 2a 2a 2a 2a 2a 2a 2a d2 3a 31 35 05 2a 2a 3a 3a 3a 3a 3a da <	4 11 7e ae 0a 0 0 0 ad 4d 2 ad 4d 2 ad 4d 2 ad 3d 2 ad 3d 2 ad 3d 2 ad 3d ad ad	8 Text Filter: 9 5 70 6e 70 2d rn: 9 6e 74 65 72 org 5 76 69 63 65 net 3 64 70 3a 64 :1	schem as-upnp- :devi ce:Inter Gatew ayDevice	Save Al Close	e He	ep	
10 00 a5 27 f5 00 00 a5 27 f5 00 a0 a0 ff a d ef a d ef a a0 a5 a1 a5 a1 a3 a1 a3 a1 a3 a5	4 11 7e ae 0a 0 0 0 ad 4d 2 ad 4d 2 ad 4d 2 ad 3d 2 ad 3d 2 ad 3d 2 ad 3d ad ad	8 Text Filter: 5 70 6e 70 2d rn: 9 6e 74 65 72 org 5 76 69 63 65 net 3 64 70 3a 64 :1:	schem as-upnp- :devi ce:Inter Gatew ayDevice ·Man: "ssdp:d	Save Al Cose	e He	ep	
10 00 a5 27 f5 00 00 a5 27 f5 00 a0 a0 ff a d ef a d ef a a0 a5 a1 a5 a1 a3 a1 a3 a1 a3 a5	4 11 7e ae 0a 0 0 0 ad 4d 2 ad 4d 2 ad 4d 2 ad 3d 2 ad 3d 2 ad 3d 2 ad 3d ad ad	8 Text Filter: 5 70 6e 70 2d rn: 9 6e 74 65 72 org 5 76 69 63 65 net 3 64 70 3a 64 :1:	schem as-upnp- :devi ce:Inter Gatew ayDevice ·Man: "ssdp:d	Save All Close	e He	eip	
010 00 a5 27 f5 00 00 0 020 ff fa d4 ef 07 6c 00 0 00 0 00 0 00 0 00 0 00 00 0 00	4 11 7e ae 0a 0 0 0 ad 4d 2 ad 4d 2 ad 4d 2 ad 3d 2 ad 3d 2 ad 3d 2 ad 3d ad ad	8 Text Filter: 5 70 6e 70 2d rn: 9 6e 74 65 72 org 5 76 69 63 65 net 3 64 70 3a 64 :1:	schem as-upnp- :devi ce:Inter Gatew ayDevice ·Man: "ssdp:d	Save Al Close	e He		94 · Daplayed: 14 (1).2%) Profile: De

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.

	n/gui/file/054ff4620aaa40928ca67a2c364bedf71d79672874d75ba50ff82	31069ad74d9/detection	🖈 🐢 t	⊫ =ı (
054ff4620aaa40928ca6	7a2c364bedf71d79672874d75ba50ff8231069ad74d9		Q 🛧 🚟 💭 Sign in	Sign
35	1) 35 engines detected this file		C	
() n	54ff4620aaa40928ca67a2c364bedf71d79672874d75ba50ff8231069ad74d9 ote.dll pedll		297.50 KB 2020-08-26 05:15:17 UTC Size 7 days ago	
DETECTION DET/	AILS RELATIONS BEHAVIOR COMMUNITY (1)			
Ad-Aware	() Gen:Variant.Zusy.311755	AegisLab	Trojan.Win32.Zusy.4lc	
Alibaba	Trojan:Win32/IcedId.fc160525	ALYac	① Trojan.lcedID.gen	
SecureAge APEX	Malicious (1) Malicious	Arcabit	Trojan.Zusy.D4C1CB	
AVG	() Win32:Malware-gen	Avira (no cloud)	() TR/AD.PhotoDlder.DD	
BitDefender	() Gen:Variant.Zusy.311755	BitDefenderTheta	() Gen:NN.ZedlaF.34196.su8@aW4giTbi	
Comodo	() .UnclassifiedMalware@0	Cyren	U W32/Trojan.OESC-3018	
			() 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
- 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.

nbns								$\times \rightarrow \cdot$
	Time	src 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>	
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>	
	2020-08-21 20:33:07.250909	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
	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>	
	2020-08-21 20:33:08.001304	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	
	2020-08-21 20:33:08.751244	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB PIZZA-BENDER<00>	
	2020-08-21 20:33:08.751462	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<00>	
	2020-08-21 20:33:08.751605	137 10.8.21.163	137	10.8.21.255	NBNS	110	Registration NB DESKTOP-OF4FE8A<20>	
	2020-08-21 20:38:11.892364	137 10.8.21.163	137	10.8.21.255	NBNS	92	Name guery NB PIZZA-BENDER<1b>	
3597 thern Des Sou Type	2020-08-21 20:38:11.892542 et II, Src: ASUSTekC_0a:f2: tination: Broadcast (ff:ff: rce: ASUSTekC_0a:f2:85 (10: e: IPv4 (0x0800)	ff:ff:ff:ff) 53:7b:0a:f2:85)	137 , Dst: Broadcast (ff:	10.8.21.163	NBNS	104	Name query response NB 10.8.21.8	
3597 Ethern ▷ Des: ▷ Sour Typ Intern 0100 0100 0100 000 15 30 00 40 45 50 46	2020-08-21 20:38:11.892542 et II, Src: ASUSTekC_09:12 tination: Broadcast (ff:ff: rce: ASUSTekC_09:12:185 [10: e: IPv4 (0x8060) et Protocol Version 4, Src: 0 = Version: 4 .0101 = Header Length: 20 ff ff ff ff ff ff ff 0: 3 7b 0 00 55 ca 00 00 80 11 f4 f ff 00 85 ea 00 00 80 11 f4 f ff 00 89 00 89 00 4c bc 9 00 000 00 00 00 12 05 45 4 45 50 46 41 43 4e 45 50 4 44 49 45 42 43 41 00 00 2	85 (10:c3:7b:0a:f2:85), ff:ff:ff:ff: (3:7b:0a:f2:85) 10.8.21.163, Dst: 10.8 oytes (5) 172 85 88 00 45 00 16 0a 08 153 00 86 16 da c28 10 00 01 16 46 64 44 54 c4 6 5 47 44 55 45 47 45 E 9 00 01 c0 c0 02 8	137 , Dst: Broadcast (ff:	10.8.21.163	NBNS	104		
3597 thern 5 Des: 5 Sour Type ntern 0104 0 ff 0 00 0 15 0 00 0 45 0 45 0 00 0 45 0 00 0 45 0 00 0 00 0 15 0 00 0 15 0 00 0 15 0 00 0 15 0 00 0 15 0 00 0 15 0 00 0 00 0 15 0 00 0 00 0 00 0 15 0 00 0	2020-08-21 20:36:11.802542 et II, Src: ASUSTekC_08:12: tination: Broadcast (ff:ff: rce: ASUSTekC_08:12:85 (10: c: IPv4 (0x0800) et Protocol Version 4, Src: 0: IPu4 (0x0800) ff:ff:ff:ff:f1 0: c3 7b 0 ff:ff:ff:ff:f1 0: c3 7b 0 ff:f6:ff:ff:f1 0: c3 7b 0 ff:f6:ff:f1 0: c3 7b 0 ff:f6:ff:f5:f6:f3:f3:f3:f3:f3:f3:f3:f3:f3:f3:f3:f3:f3:	<pre>B5 (10:c3:7b:0a:f2:85), ff:ff:ff:ff) 3:7b:0a:f2:85) 10.8.21.163, Dst: 10.8 pytes (5) 172.85 00 00 45 00 183.08 15 a3 00 06 194.08 15 a3 100 00 11 00 00 20 F 100 00 15 a3 100 00 00 00 00 100 00 00 00 00 100 00 00 00 100 00 00 00 100 00 00 00 100 00 00 00 100 00 00 100 00 00 100 00 00 100 00</pre>	137 Dst: Broadcast (ff: 3.21.255 	10.8.21.163	NBNS	194		Profile: D

Fig3.Finding hostname from NBNS traffic using wireshark

🔲 🥂 🚳 🚺 🎮 🔜 🧥 🧑 👝	⇒ ≅ 7 8 🗐 🗐 Q Q	iss Tools Help Q 聑				
http.request						×
Time	src port Source	dst port Destination	Protocol		Info	
692 2020-08-21 20:34:24.6127		80 45.12.4.190	HTTP	318 ncznw6a.com	GET /dujok/kevyl.php?l=ranec11.cab HTTP/1	1.1
1184 2020-08-21 20:34:26.7462		61208 10.8.21.163	HTTP	814	HTTP/1.1 200 OK	
6407 2020-08-21 21:23:02.7354 6409 2020-08-21 21:23:02.8429		80 8.252.146.254 61278 10.8.21.163	HTTP	341 ctidi.windowsupdate.co 381	m GET /msdownload/update/v3/static/trustedr HTTP/1.1 304 Not Modified	r/en/disa
6410 2020-08-21 21:23:02.8429		80 8.252.146.254	HTTP		m GET /msdownload/update/v3/static/trustedr	c/en/ninc
6412 2020-08-21 21:23:02.9762		61278 10.8.21.163	HTTP	389	HTTP/1.1 304 Not Modified	i /eii/piiii
7436 2020-08-21 22:23:03.9921		80 205.185.216.10	HTTP		m GET /msdownload/update/v3/static/trustedr	c/en/disa
7438 2020-08-21 22:23:04.0926		61315 10.8.21.163	HTTP	244	HTTP/1.1 304 Not Modified	, en, arsa
7439 2020-08-21 22:23:04.1036		80 205.185.216.10	HTTP	336 ctldl.windowsupdate.co	m GET /msdownload/update/v3/static/trustedr	r/en/pinr
7441 2020-08-21 22:23:04.1827	0 80 205.185.216.10	61315 10.8.21.163	HTTP	245	HTTP/1.1 304 Not Modified	1.11
GET /dujok/kevyl.php?l=ranec Accept: */*\r\n	11.cab HTTP/1.1\r\n					
Accept-Language: en-US\r\n Accept-Encoding: gzip, defla	te\r\n					
GET /dujok/kevyl.php?l=ranecc Accept: */*\r\n Accept-Language: en-US\r\n Accept-Encoding: gzip, defla User-Agent: Mozilla/4.0 (com	te\r\n	NT 10.0; WOW64; Trident/7.0; .NET4.0C	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ranec Accept: */*\r\n Accept-Language: en-US\r\n Accept-Encoding: gzip, defla	te\r\n	NT 10.0; WOW64; Trident/7.0; .NET4.0C	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ranec Accept: */*\r\n Accept-Language: en-US\r\n Accept-Encoding: gzip, defla User-Agent: Mozilla/4.0 (com Host: ncznw6a.com\r\n	te\r\n patible; MSIE 7.0; Windows H 3a 20 2a 2f 2a 0d 0a 1∙∙∕	Accep t: */*··	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ranec Accept: */*\r\n Accept-Language: en-US\r\n Accept-Encoding: gzip, defla User-Agent: Mozilla/4.0 (com Host: nczm6a.com\r\n 31 0d 0a 41 63 63 65 70 74 2d 4c 61	te\r\n patible; MSIE 7.0; Windows 1 3a 20 2a 2f 2a 0d 0a 1/ 6e 67 75 61 67 65 3a Acce	Accep t: */*·· ept-L anguage:	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ramed Accept: */*\r\n Accept-Language: en-US\r\n Accept-Encoding: grip, defla User-Agent: Nozilla/t-0 (con Host: ncznw6a.com\r\n 31 0d 0a 41 63 65 65 70 74 41 63 63 65 70 74 2d 4c 61 20 65 6e 2d 55 53 0d 0a 41	te\r\n patible; MSIE 7.0; Windows 1 3a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acco 63 63 65 70 74 2d 45 en	Accep t: */*·· ept-L anguage: -US·· Accept-E	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ranec Accept: */"\r\n Accept: acget: Maccept: acget: Jana acget: Maccept: acget: Jana acget: </td <td>te\r\n patible; MSIE 7.0; Windows 1 3a 20 2a 2f 2a 0d 0a 6e 67 75 61 67 65 3a 63 63 65 70 74 2d 45 en 7 7a 69 70 2c 22 64 ncc</td> <td>Accep t: */* ept-L anguage: -US Accept-E ding: gzip, d</td> <td>.NET4.0E)\r</td> <td>r\n</td> <td></td> <td></td>	te\r\n patible; MSIE 7.0; Windows 1 3a 20 2a 2f 2a 0d 0a 6e 67 75 61 67 65 3a 63 63 65 70 74 2d 45 en 7 7a 69 70 2c 22 64 ncc	Accep t: */* ept-L anguage: -US Accept-E ding: gzip, d	.NET4.0E)\r	r\n		
GET /dujak/kevyl.php?l=ramed Accept-language: en-US\r\n Accept-language: en-US\r\n Accept-language: en-US\r\n User-Agent: Nozilla/4.0 (con Host: nczmv6a.com\r\n 31 0d 0a 41 63 63 65 70 74 41 63 63 65 70 74 2d 4c 61 20 65 6e c3 55 38 d0 8a 41 6e 63 6f 64 69 6e 67 3a 20 65 66 6c 61 74 65 8d 0a 55	te\r\n 3a 20 2a 2f 2a 0d 0a 66 67 75 61 67 65 3a 63 63 65 70 74 2d 45 67 7a 69 70 2c 20 64 73 65 72 2d 41 67 65 efl	Accep t: */*·· ept-L anguage: -US·· Accept-E	.NET4.0E)\r	r\n		
GET /dujak/kevyl.php?l=ramed Accept:language: en-US\r\n Accept-Language: en-US\r\n Accept-Language: en-US\r\n User-Agent: Notlla/4.0 (con Host: ncrmv6s.com\r\n 10 d6 a41 65 65 76 74 24 4c 61 20 65 6c 62 55 36 d6 a41 6c 63 6f 64 69 6c 73 a2 55 66 c6 174 65 06 40 85 56 74 32 02 46 6f 7a 69 52 83 6f 64 76 174 65 62	te\r\n patible; MSIE 7.0; Windows 1 3a 20 2a 2f 2a 0d 0a 1 6e 67 75 51 67 65 3a Acce 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 20 64 ec 67 73 65 72 2d 41 67 65 efla 6c 61 2f 34 2e 30 20 nt: 6c 65 3b 20 4d 53 49 (cor	Accep t: "/" tet-L anguage: US- Accept E ding: gzip, d tet- User-Age Mozi lla/4.0 pati ble; MSI	NET4.0E)\r	r\n		
GET /dujok/kevyl.phpll=ramec Accept: Accept: git Accept: git git <tr< td=""><td>te\r\n 3a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acco 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 20 64 nco 73 65 72 2d 41 67 65 efl 6c 61 2f 34 2e 30 20 nt 6c 65 2f 34 2e 30 20 nt 6c 66 46 f7 77 3 20 4e E</td><td>Accep t: */* pt-L anguage: US- Accept-E ing: grip, d te- User-Age Mozi lla/4.0 mpati ble; MSI .0; W indows N</td><td>.NET4.0E)\r</td><td>r\n</td><td></td><td></td></tr<>	te\r\n 3a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acco 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 20 64 nco 73 65 72 2d 41 67 65 efl 6c 61 2f 34 2e 30 20 nt 6c 65 2f 34 2e 30 20 nt 6c 66 46 f7 77 3 20 4e E	Accep t: */* pt-L anguage: US- Accept-E ing: grip, d te- User-Age Mozi lla/4.0 mpati ble; MSI .0; W indows N	.NET4.0E)\r	r\n		
OET Oddigk/kevyl.php2l=ramec Accept: */*\r\m Accept-Language: en-US\r\m Accept-Language: en-US\r\m Accept-Language: en-US\r\m User-Agent: Moline J1 d0 d0 A11 63 63 570 74 24 46 61 20 65 66 c2 55 53 64 09 41 66 63 65 66 c7 34 56 66 c6 174 65 60 66 73 63 56 66 c6 174 65 60 46 35 26 36 64 09 66 74 69 62 28 23 64 67 76 69 62 26 33 26 30 72 63 30 28 39 30 28 57 56 42 08 33 02 83 30 28 05	te\r\n patible; MSIE 7.0; Windows 1 66 67 75 61 67 65 3a 66 67 75 61 67 65 3a 67 7a 69 70 22 20 64 67 7a 69 70 22 20 64 67 7a 69 70 22 20 64 66 61 2f 34 22 30 20 66 65 3b 20 4d 53 49 (cor 6e 64 6f 77 73 20 4e E 7. 4f 57 36 34 3b 20 54 T 11	Accep t: "/" ept-L anguage: US- Accept-E ding: gzip, d tac- User-Age Mozi Ila/4.0 Mozi Ila/4.0 pati ble; MSI .0; Windows N .0; WON4; T	.NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ramec Accept: #/*\r\n Accept: aguage: en-US\r\n Accept-Language: en-US\r\n Accept-Language: en-US\r\n Accept-Language: Aguage 10 del 0a 41 63 63 65 70 74 41 63 63 65 70 74 2d 4c 61 20 65 62 cd 55 53 d0 a 41 66 83 6f 64 69 66 c7 3a 20 65 66 6c 17 46 50 d0 a 55 66 74 3a 20 4d 6f 7a 69 6c 63 66 6d 70 61 74 65 06 75 24 52 03 72 29 3b 20 57 69 54 20 33 30 2e 30 3b 20 57 72 69 64 65 66 c7 43 72	te\r\n patible; MSIE 7.0; Windows I a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Accc 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 20 64 ncor 73 65 72 2d 41 67 65 efl 6c 61 2f 34 2e 30 20 nt: 6c 65 3b 20 4d 53 49 (cor 6e 64 6f 77 73 20 4e 67 4f 57 36 34 3b 20 54 T 11 30 3b 20 20 2e 4e 45 54 ridd	Accep t: */* pt-L anguage: US- Accept-E fing: grip, d tat- USer-Age Mozi lla/4.0 mpati bl; MSI 0.6; Windows N 0.6; Windows N 1.6; NRT	NET4.0E)\r	r\n		
GET /dujok/kevyl.php?l=ramec Accept: #/*\r\n Accept: aguage: en-US\r\n Accept-Language: en-US\r\n Accept-Language: en-US\r\n Accept-Language: Aguage 10 del 0a 41 63 63 65 70 74 41 63 63 65 70 74 2d 4c 61 20 65 62 cd 55 53 d0 a 41 66 83 6f 64 69 66 c7 3a 20 65 66 6c 17 46 50 d0 a 55 66 74 3a 20 4d 6f 7a 69 6c 63 66 6d 70 61 74 65 06 75 24 52 03 72 29 3b 20 57 69 54 20 33 30 2e 30 3b 20 57 72 69 64 65 66 c7 43 72	te\r\n patible; MSIE 7.0; Windows 1 6 67 75 61 67 65 3a 66 67 75 61 67 65 3a 77 8 69 70 2c 28 64 70 78 69 70 2c 28 64 65 61 2f 34 2c 38 20 nt: 6c 65 3b 28 44 53 49 (cor 6e 64 6f 77 73 24 49 7 4f 57 36 34 3b 28 54 71 130 3b 20 2e 4e 45 54 71 46 57 45 29 46 E 7 30 3b 20 2e 4e 45 54 71 46 54 36 45 29 80 4.00	Accep t: "/" ept-L anguage: US- Accept-E ding: gzip, d tac- User-Age Mozi Ila/4.0 Mozi Ila/4.0 pati ble; MSI .0; Windows N .0; WON4; T	NET4.0E)\r	r\n		
OET Oddigk/kevyl.php2l=ranec Accept: */*\rh Accept: */acque Maccept: */acque User-Agent: */acque User-Agent: */bit Maccept:	te\r\n patible; MSIE 7.0; Windows 1 a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acce 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 28 64 ncce 73 65 72 2d 41 67 65 ef1 6c 61 2f 34 2e 30 20 nt: 6c 64 6f 77 73 20 4e 2 64 6f 67 73 20 4e 54 rid 80 20 2e 4e 54 rid 73 65 29 44 53 49 (cor 74 f 57 36 34 3b 20 54 T 11 30 3b 20 2e 4e 54 54 rid 74 66 77 30 61 2e 62 76 66 32 20 76 66 63 20 00 78 66 77 36 61 2e 62 78 66 77 36 61 2e 62 78 66 77 36 66 26 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 67 78 66 78 20 78 67 78 67 78 66 78 20 78 78 77 85 78 78 78 78 78 78 78 78 78 78 78 78 78	Accep t: "/" ept-L anguage: -US- Accept E ding: grip, d tac- User-Age Mozi Ila/4.0 Mozi Ila/4.0 put ble; MSI .0; Windows N .0; WONd&T nct/7.0; .NET .1, MET4.0E)- ts. M.CZNWGA.C Conn ection:	.NET4.0E)\n	r\n		
OET Oddigk/kevyl.php2l=ranec Accept: "\"\"\" Accept: "Accept: User-Agent: "Normal State User-Agent: Normal State User-Agent: Normal State 131.04 0a.41.63.63.070 74.44.0 Host: nczmosła.com\r\n 131.04 0a.41.63.63.570 74.24.44.0 14.63.63.65.70 74.24.44.0 12.06 56.62.61.74.65 604.09.55 66.74.64.69 66.77.39.20 26.63.66.61.74.65 604.09.55 66.74.73.20.90.82.05.76 55.26 42.63.30.26.30.26.30.26.37 59.26 42.63.30.26.30.26.30.26.37 59.26 42.63.30.26.30.26.30.26.37 59.26 42.63.30.26.30.26.37 59.26 42.63.30.26.30.26.37 59.26 42.63.30.27.56 56.42 43.64.65 56.74.21 53.26.37 56.26.36 54.26.33.30.26.37 57.77 54.26.33.30.26.37 57.77 54.26.33.30.26.37 57.77 54.26.33.30.26.35 56.37 <	te\r\n patible; MSIE 7.0; Windows 1 a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acce 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 28 64 ncce 73 65 72 2d 41 67 65 ef1 6c 61 2f 34 2e 30 20 nt: 6c 64 6f 77 73 20 4e 2 64 6f 67 73 20 4e 54 rid 80 20 2e 4e 54 rid 73 65 29 44 53 49 (cor 74 f 57 36 34 3b 20 54 T 11 30 3b 20 2e 4e 54 54 rid 74 66 77 30 61 2e 62 76 66 32 20 76 66 63 20 00 78 66 77 36 61 2e 62 78 66 77 36 61 2e 62 78 66 77 36 66 26 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 67 78 66 78 20 78 67 78 67 78 66 78 20 78 78 77 85 78 78 78 78 78 78 78 78 78 78 78 78 78	Accep t: "/" pt-L anguage: US- Accept-E ing: grip, d te: User-Age Mozi lla/4.0 puti ble: MSI .0; W indows N .0; W indows N .0; WON64; T mct/7.0; NET ; N ET4.0E).	.NET4.0E)\r	r\n		
OET Oddigk/kevyl.php2l=ranec Accept: */*\rh Accept: */acque Maccept: */acque User-Agent: */acque User-Agent: */bit Maccept:	te\r\n patible; MSIE 7.0; Windows 1 a 20 2a 2f 2a 0d 0a 1 6e 67 75 61 67 65 3a Acce 63 63 65 70 74 2d 45 en 67 7a 69 70 2c 28 64 ncce 73 65 72 2d 41 67 65 ef1 6c 61 2f 34 2e 30 20 nt: 6c 64 6f 77 73 20 4e 2 64 6f 67 73 20 4e 54 rid 80 20 2e 4e 54 rid 73 65 29 44 53 49 (cor 74 f 57 36 34 3b 20 54 T 11 30 3b 20 2e 4e 54 54 rid 74 66 77 30 61 2e 62 76 66 32 20 76 66 63 20 00 78 66 77 36 61 2e 62 78 66 77 36 61 2e 62 78 66 77 36 66 26 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 66 77 36 66 78 20 78 67 78 66 78 20 78 67 78 66 78 20 78 67 78 67 78 66 78 20 78 78 77 85 78 78 78 78 78 78 78 78 78 78 78 78 78	Accep t: "/" ept-L anguage: -US- Accept E ding: grip, d tac- User-Age Mozi Ila/4.0 Mozi Ila/4.0 put ble; MSI .0; Windows N .0; WONd&T nct/7.0; .NET .1, MET4.0E)- ts. M.CZNWGA.C Conn ection:	.NET4.0E)\r		4 · Displayed: 10 (0. 1%)	Profile: De

Fig 4 finding domain address using wireshark

le E	0-08-21-tr	affic-analysis-exerc	ise.pcap		-	- D				
	Edit Viev	w Go Capture	Analyze	Statistics	5 Telephony	Wireless Tools Help				
	1	퉬 🔚 🔀 🞑	۹ 🗢 ه	😫 🗧		Q Q Q II				
http.	.request									
	Time			src port	Source	dst port	Destination	Protocol	Length Host	Info
	8 2020	-08-21 20:33:0	6.624945	54511	10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
	11 2020	-08-21 20:33:0	6.923092	54511	10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
	70 2020	-08-21 20:33:0	7.908598	54511	10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
1	150 2020	-08-21 20:33:0	9.640765	54511	10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
2	208 2020	-08-21 20:33:1	0.908359		10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
2	216 2020	-08-21 20:33:1	3.908271		10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
		-08-21 20:34:24			10.8.21.163	80	45.12.4.190	HTTP	318 ncznw6a.com	GET /dujok/kevyl.php?l=ranec11.cab HTTP/1.1
		-08-21 20:41:0			10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
		-08-21 20:41:0			10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
		-08-21 20:41:0			10.8.21.163	1900	239.255.255.250	SSDP	179 239.255.255.250:1900	M-SEARCH * HTTP/1.1
		-08-21 21:23:0			10.8.21.163	80	8.252.146.254	HTTP		m GET /msdownload/update/v3/static/trustedr/en
		-08-21 21:23:0			10.8.21.163	80	8.252.146.254	HTTP		m GET /msdownload/update/v3/static/trustedr/en
		-08-21 22:23:0			10.8.21.163	80	205.185.216.10	HTTP		m GET /msdownload/update/v3/static/trustedr/en
74	439 2020	-08-21 22:23:0	4.103630	61315	10.8.21.163	80	205.185.216.10	HTTP	336 ctldl.windowsupdate.co	m GET /msdownload/update/v3/static/trustedr/en
	Source:	checksum statu 10.8.21.163		ified]						
		tion: 45.12.4.1								
ra	ansmissio	on Control Prot	tocol, Sr	c Port:	61208, Dst F	Port: 80, Seq: 1, Ack: 3	1, Len: 264			
0	01 30 8	Sc 09 40 00 80	06 1c 4	a 0a 08	15 a3 2d Oc	.0@] <mark></mark>				
0		ef 18 00 50 15				•••••P•[•••}•TP•				
		31 9e 00 00 47				··1···GE T /dujok				
		5 76 79 6c 2e		0 3† 6c	3d 72 61 6e	/kevyl.p hp?l=ran				
0					50.05.00.0					
0	65 63 3	31 31 2e 63 61				ec11.cab HTTP/1.				
0 0	65 63 3 31 0d 0	a 41 63 63 65	70 74 3	a 20 2a	2f 2a 0d 0a	ec11.cab HTTP/1. 1 Accep t: */*··				
0 0 0	65 63 3 31 0d 0 41 63 6		70 74 3 4c 61 6	a 202a e 6775	2f 2a 0d 0a	ec11.cab HTTP/1.				
0 0 0 0	65 63 3 31 0d 0 41 63 6 20 65 6	a 41 63 63 65 3 65 70 74 2d	70 74 3 4c 61 6 0a 41 6	a 20 2a e 67 75 3 63 65	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45	ec11.cab HTTP/1. 1…Accep t: */*… Accept-L anguage:				
0 0 0 0 0 0	65 63 3 31 0d 0 41 63 6 20 65 6 6e 63 6 65 66 6	a 41 63 63 65 53 65 70 74 2d 56 2d 55 53 0d 57 64 69 6e 67 56 61 74 65 0d	70 74 3 4c 61 6 0a 41 6 3a 20 6 0a 55 7	a 20 2a e 67 75 3 63 65 7 7a 69 3 65 72	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45 70 2c 20 64 2d 41 67 65	ec11.cab HTTP/1. 1Accep t: */* Accept-L anguage: en-US Accept-E ncoding: gzip, d eflate User-Age				
000000000000000000000000000000000000000	65 63 3 31 0d 0 41 63 6 20 65 6 6e 63 6 65 66 6 6e 74 3	a 41 63 63 65 is 65 70 74 2d is 2d 55 53 0d if 64 69 6e 67 ic 61 74 65 0d	70 74 3 4c 61 6 0a 41 6 3a 20 6 0a 55 7 69 6c 6	a 20 2a e 67 75 3 63 65 7 7a 69 3 65 72 c 61 2f	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45 70 2c 20 64 2d 41 67 65 34 2e 30 20	ec11.cab HTTP/1. 1Accep t: */* Accept-L anguage: en-USAccept-E ncoding: gzip, d eflateUser-Age nt: Mozi lla/4.0				
0 0 0 0 0 0 0 0 0 0 0 0 0	65 63 3 31 0d 0 41 63 6 20 65 6 6e 63 6 65 66 6 6e 74 3 28 63 6	a 41 63 63 65 i 65 70 74 2d i 2d 55 53 0d i 64 69 6e 67 ic 61 74 65 0d ia 20 4d 67 7a ia 20 4d 67 7a ia 60 70 61 74	70 74 3 4c 61 6 0a 41 6 3a 20 6 0a 55 7 69 6c 6 69 62 6	a 20 2a e 67 75 3 63 65 7 7a 69 3 65 72 c 61 2f c 65 3b	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45 70 2c 20 64 2d 41 67 65 34 2e 30 20 20 4d 53 49	ec11.cab HTTP/1. 1Accep t: */* Accept-L anguage: en-USAccept-E ncoding: gzip, d eflateUser-Age nt: Mozi lla/4.0 (compati ble; MSI				
0 0 0 0 0 0 0 0 0 0 0 0 0	65 63 3 31 0d 0 41 63 6 20 65 6 6e 63 6 6e 74 3 28 63 6 45 20 3	a 41 63 63 65 33 65 70 74 2d 52 2d 55 53 0d 56 64 69 6e 67 56 61 74 65 0d 56 20 40 67 36 57 20 40 67 74 58 20 40 67 74 59 20 40 67 74 50 20 30 50 70 50 20 30 50 20	70 74 3 4c 61 6 0a 41 6 3a 20 6 0a 55 7 69 6c 6 69 62 6 57 69 6	a 20 2a e 67 75 3 63 65 7 7a 69 3 65 72 c 61 2f c 65 3b e 64 6f	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45 70 2c 20 64 2d 41 67 65 34 2e 30 20 20 4d 53 49 77 73 20 4e	ec11.cab HTTP/1. 1Accep t: */* Accept-L anguage: en-US Accept-E ncoding: gzip, d eflate User-Age nt: Mozi lla/4.0 (compati ble; MSI E 7.0; W indows N				
10 50 70 50 50 50 50 50	65 63 3 31 0d 0 41 63 6 6e 63 6 6e 63 6 6e 74 3 28 63 6 45 20 3 54 20 3	a 41 63 63 65 i 65 70 74 2d i 2d 55 53 0d i 64 69 6e 67 ic 61 74 65 0d ia 20 4d 67 7a ia 20 4d 67 7a ia 60 70 61 74	70 74 3 4c 61 6 0a 41 6 3a 20 6 0a 55 7 69 6c 6 69 62 6 57 69 6	a 20 2a e 67 75 3 63 65 7 7a 69 3 65 72 c 61 2f c 65 3b e 64 6f	2f 2a 0d 0a 61 67 65 3a 70 74 2d 45 70 2c 20 64 2d 41 67 65 34 2e 30 20 20 4d 53 49 77 73 20 4e	ec11.cab HTTP/1. 1Accep t: */* Accept-L anguage: en-US Accept-E ncoding: gzip, d eflate User-Age nt: Mozi lla/4.0 (compati ble; MSI E 7.0; W indows N			Padets: 789	4 · Displayed: 14 (0,2%)

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" 2nd 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