

Forensic Tool for Wireless Surveillance Camera

Reem Alshalawi, Turki Alghamdi

College of Computer and Information System, Umm Al-Qura University, Kingdom of Saudi Arabia

rmshalawi@uqu.edu.sa , taghamdi@uqu.edu.sa

Abstract— Nowadays, there is a stringent need for smart technology such as surveillance camera. Although these technologies can improve people's life they are not failure proof and can be hacked, leading to various threats. In this research, we present a new tool in network forensic. We investigate the possible illegal access (attack) on wireless surveillance camera. This proposed tool is designed into two stages. First, a new monitoring scheme is built to keep the privacy of data. Second, investigation process that plays a big role for saving users' privacy and highly secure places that use surveillance camera is facilitated. The analysis results obtained indicates that the proposed approach has a high efficiency and can be easily used to determine attacks.

Keywords— Privacy, Network Forensic, Surveillance Camera, Wireless Network, Forensic Tool

I. INTRODUCTION

Nowadays, many electronic devices depend on internet access to perform various tasks. Therefore, the value of these devices is associated with the connection availability. One of the latest technologies that concerns internet connectivity is represented by the Wireless Networks (WLAN), its adoption being widely accepted and it has many advantages [1]. There are multitude systems with wireless connections, in this work, the focus being on the wireless camera, which is one of the devices vulnerable to the threat of unauthorized access. Such a scenario is a nightmare for those who rely on it, especially in surveillance or high privacy places. Consequently, having conclusive evidences against the attacker of wireless camera is required for both the victim(s) and court. These software forensic applications are being influential on both social and economic aspects of video surveillance. The explosion of WLAN use opened the door for many crimes: eye teasing, child pornography, harassing personal lives, threatening via mobile phones, stealing personal data or credit passwords etc..

Until no standard wireless network forensic framework was developed, this will continue. Consequently, crime analysis is very difficult [2]. In addition, there are not enough analysis tools, softwares and documentations regarding those crimes and forensic analysis. Therefore, there is a strong need for developing efficient tools which achieve the required results in a fast, intuitive and easy manner.

As computer and other digital devices became more common, investigators had to consider evidences substantiating crimes stored in these devices too. This leads to the development of cyber forensic tools for acquiring and

analyzing digital evidences. Unfortunately, with these forensic tools, there are a series of problems related to: i) source identification in case of wireless loss networks [3]; ii) a high requirement of rapid software development; iii) the need to incorporate changes in the representation of available input data. In addition, sometimes customers report an important requirement at a later development stage. All these issues pose challenge to the normal functioning of the team and impede the classical implementation plan and software development process [4].

Wireless network forensics is a branch of computer forensics which deals with the forensic analysis of live or captured computer network traffic [5]. This analysis may be aimed at detecting possible intrusions, collecting and gathering information and evidence about suspected attacks. All the information flowing on various network channels, regardless of its type (wireless, wired or fiber optic), is essentially volatile and dynamic in nature. For effective forensic analysis and later usage in a court of law as evidence, the traffic is required to be stored and then analyzed [6]. Network monitoring and software analysis have increasingly become more sophisticated and potent with the passage of time. There are two locations where a network analysis and monitoring tool can be employed: on the host and/or on the network. For both these categories of monitoring, there are different tools such as Tcpdump, Tshark, Tcpextract and Wireshark.

Many network forensic analysis techniques and tools were developed and employed for intrusion detection and collection of evidence. Some of these tools are Tcpdump, Wireshark, TShark and Tcpextract [7-8] but these are general approaches and are not especially developed for the problems specific to camera WiFi. Due to transient and volatile nature of the network traffic, forensic analysis requires a pro-active approach.

What concerns the wireless cameras is the majority of approaches tackle problems related to the mobile devices with incorporated cameras [9, 10]. On the other hand, for wireless closed circuit television (CCTV) usually used for surveillance, there are fewer works. The most comprehensible one is the one of Cole at al. [11]. It was concluded that, along with the vulnerabilities of classical IP based CCTVs (exposure to IP based vulnerabilities), the wireless CCTVs have a series of problems related to: remote, physical denial of service attacks due to the broadcast system, interception of traffic, protocol

vulnerabilities (layer 1- physical jamming-availability, layer 2 – logical jamming) and lack of power.

In this work, a forensic tool for wireless surveillance cameras is proposed. It is based on a detailed analysis of the network traffic for a given hardware configuration.

II. PROPOSED APPROACH

We investigate the possible illegal access (attack) on wireless surveillance camera. This proposed tool is designed into two stages. First, a new monitoring scheme is built to keep the privacy of data. Second, the investigation process that plays a big role for saving users’ privacy and highly secure places that use surveillance camera is facilitated.

This developed tool runs under certain circumstances and is designed to work when it is attached to the complete system, which we call a model. This model consists of a default Gateway (G), an IP Surveillance Camera, both having static IP address, and a trusted PC.

G works as a monitoring unit that watches all network traffics using wireshark. It is connected to the backup server (BS). Every period of time (t), the BS checks G that sends the capture files to the BS (Figure (1)). G and BS are run on the same network. Thus, for security issues, we transfer copies of all capture files to

BS that has a log file which records all copied information (date, size, etc...), if BS does not receive any copy this indicate for attack.

The gateway of the surveillance camera is set to G (Figure (2)). The network communicates with the IP camera and G. The IP camera traffic passes only through G and it can read, capture, and analyze. The destination of this traffic is the trusted PC. The specifications of the IP camera are illustrated in Table 1.

The trusted PCs are the only devices allowed to have a legal access to the camera. Trusted PCs also are allowed to connect to each other (authorized access). See figure (3).



Figure 1. Gateway G and Backup Server BS



Figure 2. Gateway G and Wireless Camera

TABLE 1. The Specification of the Wireless Camera [12]

Model		UDP: 11H-102B-B10
Device	Device Type	1.0 Megapixel CMOS Sensor 1/4"
	Day&Night	Yes
	Color	0.5Lux (IR ON)
	IR Cut Filter	Support
Lens	IR Distance	8-10MvVVC
	Lens	3.6MM
	IRIS	Fixed Aperture F1.2
	Viewing Angle	Pan: 355°/Tilt: 90°
Video	Compression	H.264
	Resolution & Frame	Main Flow: 1280*720@30fps Minor Flow: 640*360@30fps
	Code Stream	Support Dual Stream
	Code Rate	32-4096Kbps
	Bit Rate Type	CBR & VBR
	SNR	Above 50DB
Alarm	Audio	1 CH Two-way-audio Built-in Mic External Output Device
	Alarm In/ Out	1CH
	Ethernet Port	Ethernet (10/100 Base-T), RJ-45 connector
Software	Intelligent Software Function	Motion Detect, Miss Object Detection, Suspicious Detection, Moving Object Tracking, Guard Line Detection, etc.
	Event Action	Video Capture Saved to Backing Device, Send Email, Send SMS, Zoom in alarm, Pop up map, Go to PTZ preset pos etc.
	Remote Access	DDNS, software, P2P
	Power Consumption	DC 5V/2A
General	Operation Temperature	-10°C ~60°C
	Operation Humidity	10%-80%
	Dimensions	103(L)*75(W)*125(H)mm

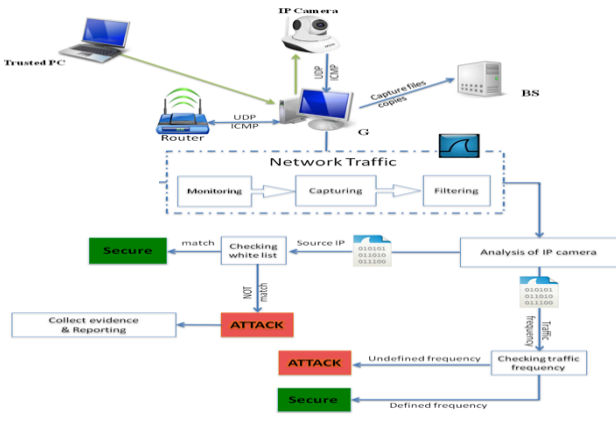


Figure 3. Tool Design Overview

2.1 Monitoring Network Traffic

G monitors the traffic using the Wireshark application. Wireshark has features that facilitate monitoring, capturing, and filtering the traffic (see Figure 3). The movement of the camera packets and trusted PC packets are traced out as shown in Figure (4). Every packet has data stored in one row and six columns which are No. (refers to the row number), Time (refers to the sending time duration), Source (indicates the source IP address), Destination (indicates the destination IP address), Protocol, and length info. In the analysis, we focus on the first three columns (No., Time, and Source).

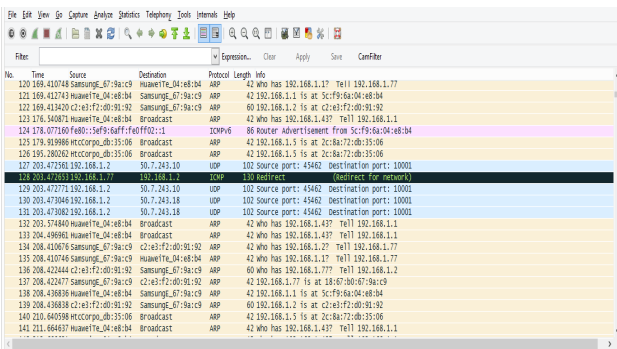


Figure 4. Monitoring in Gateway G

2.2 Monitoring Network Traffic

Wireshark is running all the time. The data that we need cannot be read directly from Wireshark, the tool needs to capture and filter them. We use Wireshark filter to get the desirable data. The command in Figure (5) is used to filter unnecessary traffic associated with the IP address of the camera 192.168.1.2 and to extract the capture file of certain IP address:

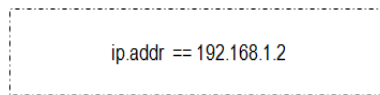


Figure 5. Filter Syntax

2.3 Analysis of Captured File

The process of analysis starts after filtering the network traffic and exporting in a CSV format. The process of analyzing the wireless camera traffic is done into two cases.

In the first case, the analysis is done by checking and comparing the source IP in IP camera capture file with the white list that contains a group of authorized IP addresses to access IP camera and consider the trusted machine that is not suspicious. If the result of the comparison matches any IP in the white list this means there is no attack. Otherwise, if the result of the comparison does not match any IP in the white list, then an attack by unauthorized access occurred and the file containing the row information is exported to the investigator. See Figure (6).

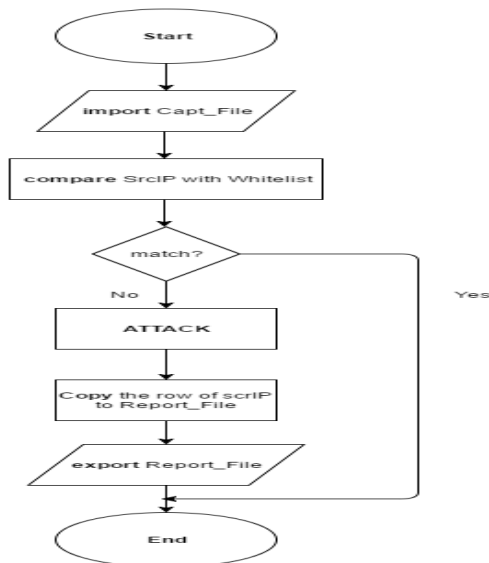


Figure 6. Flowchart of Compared Source IP

In the second case, the analysis is done by checking and comparing the time. We focus on the time the packet is sent, information which is stored in the second column. We calculate the difference of every two rows and we compare the result of difference with the time factor (tf).

For example, if we are calculating the differences of row 4 and 5, such: row 4 (time) – row 5 (time) = difference time (dt) this dt compared with tf. Then, the mean value of the sending packet is computed, and considered as tf. Based on the default

situation in which the camera works 24 hours, if there is a miss in time of sending packet, this means there is an attack occurring. On the other hand, if there are no more packets from camera, then the camera gateway is changed and we cannot watch it. Consequently, all recent and last transactions of the camera will be reported to the investigator. Figure (7) shows the flowchart of camera sending time analysis.

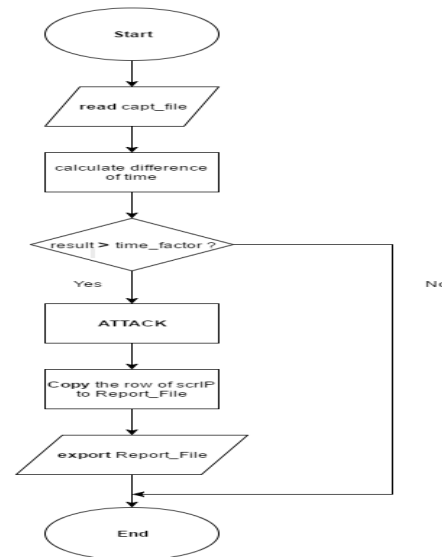


Figure 7. Flowchart of Camera Transmit Time Calculating

III. CASE STUDY

The experiments in this study are done by using Household IP camera HD Network camera (UXD Mega-pixel UIP-IHF 1028-B10 LEN:2.8MM LENS Adapter Power:5V/2A), The Wireshark Network Analyzer Version 1.12.8 (v1.12.8-0g5b6e543 from master-1.12), Microsoft Windows 8 64bit as operating system, with the processor Intel(R) Core(TM) i3-3120M CPU @ 2.50GHz, and RAM: 4,00 GB.

As seen in (Figure 3) and (Figure 4), while we monitor camera traffic through Wireshark, we capture camera transactions and export it in capture file with csv format, then to drop unnecessary data by using Wireshark filter see (Figure 5). Camera capture file of this case study consists 835 lines then we analyze this capture file with two algorithms (Figure 6) and (Figure 7). First, we compare source IP in capture file with IP listed in the whitelist to record secure case as "match" and attack case as "NOT match".

Second, calculating camera transmits time. Then, each transmit time compared with tf to detect attack case.

IV. RESULT AND ANALYSIS

All of the experiments use confusion matrix rates to evaluate the performance, and we compute true positive (TP), true negative (TN), false positive (FP), and false negative (FN). TP means the result of matching is secured when it is in real state it matches any IP address in the white list, and the

result of matching is attacked when it is in not real state it doesn't match any IP address in the white list. FP means the result of matching is secured but it is in real "NOT match" state, any IP address in the white list will do, or the result of matching is attacked but in real "match" state any IP address in the white list will not there is no shown result of attack case in real state, or there is no shown result for secure case in real state. FN means there is no result of any wrong matching analysis. All these rates are used to acquire the result of our measurements; precision, recall, and accuracy.

A. COMPARED SOURCE IP (CSIP)

The purpose of this analysis is to record the attack information on camera when we find not matching for any IP address in the white list with the capture file. The analysis here focuses on the source IP address, which is compared with the white list. The results are shown in Table 2.

TABLE 1. Result of CSIP Camera Capture File from Case Study

Line	Source IP	White List	Result	TP	FP	TN	FN
4	192.168.1.2	192.168.1.77	Match	1	0	0	0
5	192.168.1.2		Match	1	0	0	0
7	192.168.1.2		Match	1	0	0	0
8	192.168.1.2		Match	1	0	0	0
10	192.168.1.77	192.168.1.2	Match	1	0	0	0
56	192.168.1.2		Match	1	0	0	0
57	192.168.1.77	192.168.1.6	Match	1	0	0	0
58	192.168.1.2		Match	1	0	0	0

$$\text{Precision} = \frac{TP}{TP+FP} = \frac{835}{835+0} = 1$$

$$\text{Recall} = \frac{TP}{TP+FN} = \frac{835}{835+0} = \frac{835}{835} = 1$$

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} = \frac{835}{835} = 1$$

TP, TN, FP and FN values from Table 2.

As it can be observed, precision and recall and accuracy are equal. This refers to powerful potential provided by our proposed tool. This means that the proposed tool provides a high accuracy, precision and recall. The reason behind this high rate is the Wireshark filter. We have seen the filter before in 2.2 and the analytical side using match algorithm with accurate whitelist. When we are looking for count, all matched IP address and our algorithm can count it accurately as well as counting not match IP address. Our tool grants there is no miss-match result while the whitelist up to date and the last one is responsible for network admin.

B. Camera Transmit Time Calculating (CTTC)

We calculate the mean of time for packets from case study capture file to determine attack case. Figure (8) shows the time record of the camera capture file in our case study. We calculate the mean of camera capture file and the results of analysis shown in Table 3. The camera capture file mean is 3.030045917, so we can consider $t_f = 4.8$.

	B	A	
0.000099000	276.588307000	276.588208000	23
0.001547000	276.590770000	276.588223000	24
0.000604000	276.591391000	276.590787000	25
2.278766000	276.870169000	276.591403000	26
0.000124000	316.524810000	316.524868000	27
0.000210000	316.525185000	316.524975000	28
0.305950000	316.831173000	316.525223000	29
0.000145000	356.256275000	356.256130000	30
0.001463000	356.257988000	356.256525000	31
0.000553000	356.258571000	356.258018000	32
3.094441000	359.328032000	356.258591000	33
0.000088000	384.913404000	384.913316000	34
0.000296000	384.913822000	384.913528000	35
5.170321000	400.084182000	384.913861000	36
0.000147000	434.900821000	434.900774000	37
0.001479000	434.902711000	434.901232000	38

Figure 8. The Mean of CTTC from Case Study

TABLE 2. CTTC of Camera Capture File from Case Study

Time	Factor	Result	TP	FP	TN	FN
0.000099000	4.8	Secure	1	0	0	0
0.001547000		Secure	1	0	0	0
0.000604000		Secure	1	0	0	0
2.278766000		Secure	1	0	0	0
0.000124000		Secure	1	0	0	0
0.000210000		Secure	1	0	0	0
7.105580000		ATTACK	0	1	0	0
19.453932000		ATTACK	0	1	0	0
3.069441000		Secure	1	0	0	0
3.023072467		Secure	1	0	0	0
13.031007152		ATTACK	0	1	0	0
3.010107200		Secure	1	0	0	0
0.004417843		Secure	1	0	0	0
0.000102103		Secure	1	0	0	0

$$\text{Precision} = \frac{TP}{TP+FP} = \frac{832}{832+3} = 0.99640719$$

$$\text{Recall} = \frac{TP}{TP+FN} = \frac{832}{832+0} = \frac{832}{832} = 1$$

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} = \frac{832+0}{832+3+0+0} = 0.99640719$$

TP, TN, FP, and FN from Table 3.

From the above results we can conclude that our tool can perform high rates in performance measurements with well defined hardware and software specification.

V. CONCLUSIONS

The objectives of this research were to develop a monitor scheme that facilitates the way of acquiring the evidences without preaching privacy of the data and to facilitate the process in which investigators collect, examine, and analyze the evidence. The proposed approach is based on a specific hardware configuration where Wireshark runs on gateway G to monitor camera and the trusted PC traffic and to preserve the data. Then, G sends the backup of capture files to server BS. The analysis of capture files starts filtering the data in order to determine the traffic belonging to the surveillance camera. The camera traffic was analyzed from two perspectives.

First, the unauthorized IP which illegally accessed surveillance camera was analyzed. To be able to do that, all source IP in camera capture file were read and compared. The comparison is done between the source IP and the whitelist. This analysis had a high performance, fact which was

indicated by the high accuracy, recall, and precision. The second approach consist of finding the lost time of surveillance camera transactions in which any missing packet indicates that there is an attack on surveillance camera. The results have a recall score of 100%, and precision and accuracy scores of 99%. This facilitates monitoring surveillance camera incoming and outgoing traffic by time.

REFERENCES

- [1] W. Lehr and L. W. McKnight, "Wireless internet access: 3G vs. WiFi?," Telecommunications Policy, vol. 27, no. 5, pp.351-370, 2003.
- [2] "Security architecture." www.educause.edu/.../pdf/PUB7 . 2015.
- [3] S. Chen, A. Pande, K. Zeng et al., "Live Video Forensics: Source Identification in Lossy Wireless Networks," 2013.
- [4] C. Balan, S. Dija, and D. S. Vidyadharan, "The need to adopt agile methodology in the development of cyber forensics tools." Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on , pp. 1-4, 2010. IEEE.
- [5] "Develop a comprehensive network security plan." <http://www.techrepublic.com/resource-library/whitepapers/develop-a-comprehensive-network-security-plan/> . 2015.
- [6] "File carving with ProDiscover Basic." <http://digital-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager> . 2015.
- [7] L. A. Chappell and G. Combs, Wireshark network analysis: the official Wireshark certified network analyst study guide: Protocol Analysis Institute, Chappell University, 2010.
- [8] G. Combs, "TShark- Dump and Analyze Network Traffic." . 2012. Wireshark.
- [9] G. An, D. Seo, J. Kim et al., "Context-based remote security control for mobile communication device." Communications and Information Technologies (ISCIT), 2010 International Symposium on , pp. 815-820, 2010. IEEE.
- [10] N. Husted, H. Saidi, and A. Gehani, "Smartphone security limitations: conflicting traditions." Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies , pp. 5-12. 2011. ACM.
- [11] M. Coole, A. Woodward, and C. Valli, "Understanding the Vulnerabilities in Wi-Fi and the Impact on its Use in CCTV Systems," 2012.
- [12] "UIP-IHF1028-B10 - UXD Technologies Ltd.", UXD Technologies Ltd., 2016. [Online]. Available: <http://www.uxdsecurity.com/product-detail/uiib-ihf1028-b10/>.

Reem M. Alshalawi is currently a graduate student, pursuing Master of Sciences (MS) degree in Computer Sciences & Engineering, at Umm Al-Qura University (UQU)

In 2011, Reem completed her Bachelor of Sciences (BS) degree from UQU Saudi Arabia. Reem followed her BS studies by pursuing a higher diploma degree in education in 2012 and higher diploma in measurement and evaluation from UQU completed by the end of 2013.

Turki A. Alghamdi Assistant Professor in Computer Science Department, faculty of Computer and Information Systems, University of Umm Al-Qura (UQU) in Makkah, Saudi Arabia.

He holds a B.Sc. in computer science. He was awarded M.Sc. degree in



Distributed Systems and Networks from the University of Hertfordshire, Hatfield in 2006. In 2010 he received his Ph.D. degree in Computer Networks from the University of Bradford, Bradford, United Kingdom.

After five years at UQU IT deanship as a Vice Dean for Technical affairs, Dr. Alghamdi joined the Taif University in 2016 as a Dean of IT, eLearning & Distance Education.

He is holder of CDCDP and CDCMP certificates. He is passionate about developing the translational and collaborative interface between industry and academia. His current research interests include Wireless Sensor Networks, Energy and QoS Aware Routing Protocols, Network Security and Distributed Systems.

University.