

دليل شامل لأداة Wireshark الجزء الثاني

مرحباً بك في الدليل المتقدم لأداة Wireshark، حيث ستتعلم تقنيات التحليل المتقدمة، الأوامر الكاملة، والأسرار التي تجعلك خبيراً في تحليل حركة الشبكة.



رسوم بيانية

تصورات متقدمة، تحليلات مرئية، وتقارير تفصيلية



تحليل أمني

كشف الهجمات، تحليل التهديدات، وحماية الشبكات



أوامر كاملة

فلاتر متقدمة، أوامر خطية، واختصارات لتحليل فعال



أسرار احترافية

نصائح الخبراء، تقنيات متقدمة، وأفضل الممارسات



تحليل متقدم

بروتوكولات معقدة، حركة مشفرة، واستكشاف أخطاء



مهام عملية

تمارين واقعية، سيناريوهات تطبيقية، وحالات دراسية

من إعداد: أ. عبد الصمد بوركيبات

باحث في فقه الأمن السيبراني الأسري، ومتخصص في الأمن السيبراني



مرجع أوامر Wireshark الشامل

فلتر الالتقاط، فلتر العرض، العوامل المنطقية، واختصارات لوحة المفاتيح

فلتر العرض

النوع	مثال
عنوان IP	<code>ip.addr == 192.168.1.1</code>
عنوان المصدر	<code>ip.src == 192.168.1.1</code>
عنوان الوجهة	<code>ip.dst == 192.168.1.1</code>
المنفذ	<code>tcp.port == 80</code>
البروتوكول	<code>tcp or http</code>

فلتر الالتقاط

النوع	مثال
عنوان IP	<code>host 192.168.1.1</code>
منفذ TCP/UDP	<code>tcp port 80</code>
نطاق IP	<code>net 192.168.1.0/24</code>
بروتوكول	<code>tcp or udp</code>
عنوان MAC	<code>ether host 00:0c:29:12:34:56</code>

اختصارات لوحة المفاتيح

Ctrl+E ▶ - بدء/إيقاف الالتقاط	Ctrl+F ▼ - البحث في الحزم
Ctrl+↓ - الحزمة التالية	Ctrl+↑ - الحزمة السابقة
Ctrl+N 🏠 - الانتقال إلى الحزمة	Ctrl+S 💾 - حفظ الالتقاط
Ctrl+Shift+C ✎ - تلوين الحزم	Ctrl+O 📄 - فتح ملف

نصيحة:

استخدم ! للنفي في فلتر العرض، مثال: `tcp!` لعرض جميع الحزم غير TCP

العوامل المنطقية والمقارنة

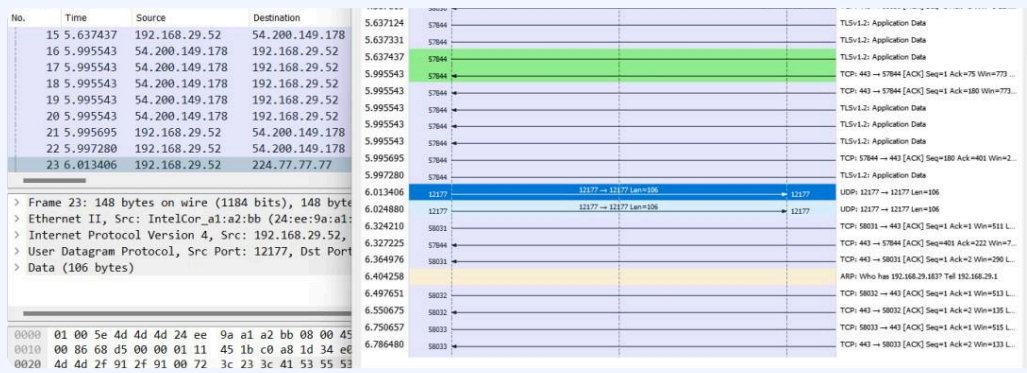
العامل	الوصف	مثال
and	منطقي AND	<code>ip.addr == 192.168.1.1 and tcp.port == 80</code>
or	منطقي OR	<code>tcp.port == 80 or tcp.port == 443</code>
==	يساوي	<code>ip.addr == 192.168.1.1</code>
!=	لا يساوي	<code>ip.addr != 192.168.1.1</code>

تقنيات التحليل المتقدمة

متابعة تدفقات البروتوكول، تحليل TCP، إعادة تجميع الحزم، وتحليل المعلومات الخبيثة

تحليل TCP وإعادة التجميع

- ✓ **TCP Flags**: تحليل SYN, ACK, FIN, RST
- ✓ **Sequence/Ack**: تتبع أرقام التسلسل والتأكيد
- ✓ **Retransmission**: كشف إعادة الإرسال
- ✓ **Window Size**: تحليل حجم النافذة

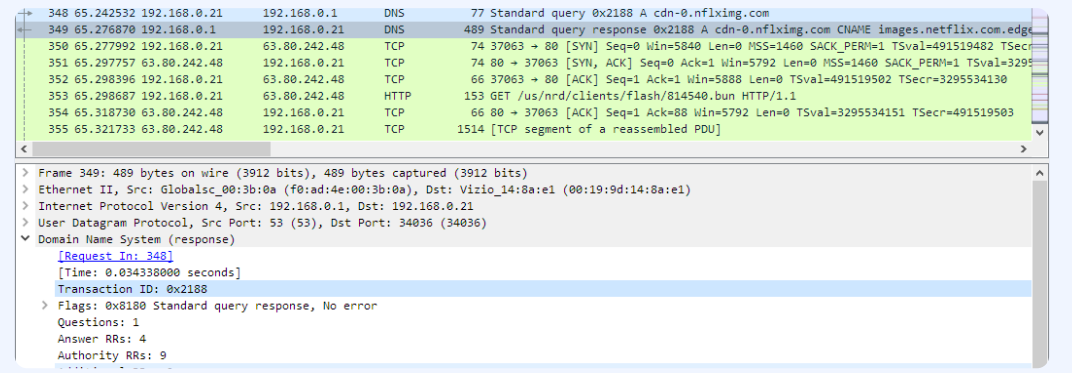


نصيحة

تفعيل **TCP Analysis** من **Expert Info** → **Analyze** لكشف المشاكل

متابعة تدفقات البروتوكول

- ✓ **TCP Stream**: تحليل اتصالات TCP الكاملة
- ✓ **HTTP Stream**: عرض طلبات وردود HTTP
- ✓ **SSL/TLS**: فك تشفير الجلسات المشفرة
- ✓ **UDP Stream**: تحليل تدفقات UDP

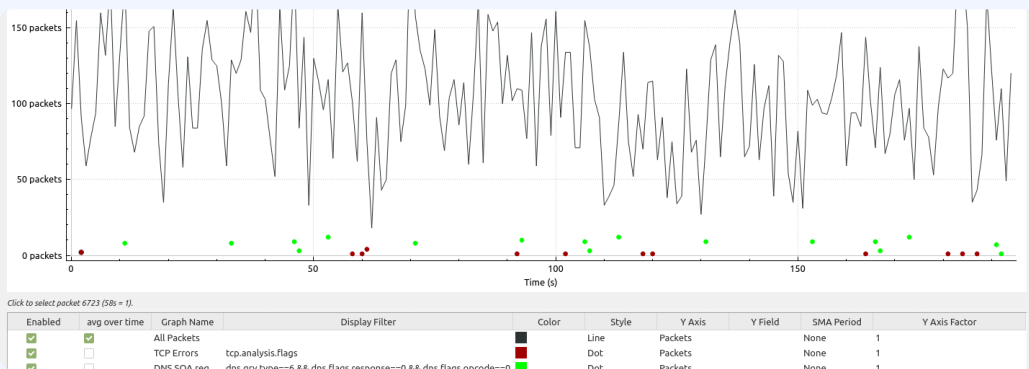


نصيحة

استخدم **TCP Stream** → **Follow** → **Analyze** لعرض محادثة TCP كاملة

تحليل المعلومات الخبيثة

- ✓ **Expert Info**: عرض المشاكل والتحذيرات
- ✓ **Colorization**: تلوين الحزم حسب الأهمية
- ✓ **Notes**: إضافة ملاحظات للحزم
- ✓ **Comments**: إضافة تعليقات للتحليل

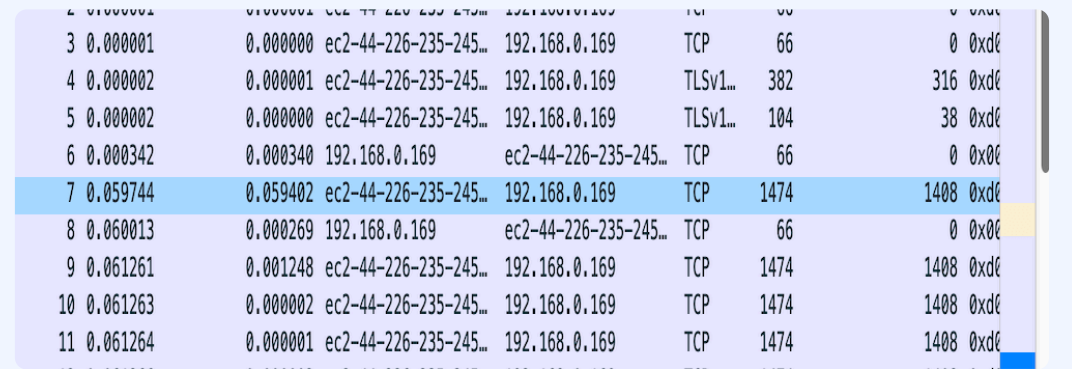


نصيحة

تفعيل **Coloring Rules** → **View** لتخصيص ألوان الحزم

تقنيات إعادة تجميع الحزم

- ✓ **IP Defragmentation**: إعادة تجميع أجزاء IP
- ✓ **TCP Reassembly**: إعادة تجميع شرائح TCP
- ✓ **SMB Reassembly**: إعادة تجميع ملفات SMB
- ✓ **HTTP Objects**: استخراج كائنات HTTP



نصيحة

استخدم **HTTP Objects** → **Export Objects** → **File ...** لاستخراج الملفات

تحليل الأمان مع Wireshark

كشف عمليات المسح، هجمات ARP، تحليل البرامج الضارة، وفك تشفير جلسات SSL/TLS

كشف هجمات ARP و MITM

- ✓ **ARP Poisoning**: تزوير عناوين MAC
- ✓ **Duplicate ARP**: استجابات ARP مكررة
- ✓ **gratuitous ARP**: حزم ARP غير مطلوبة
- ✓ **MITM**: اعتراض وتحويل حركة المرور

No.	Time	Source	Destination	Protocol	Info
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=&ncp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

فلتر كشف ARP غير طبيعي

arp.duplicate-address-detected

كشف عمليات مسح Nmap

- ✓ **TCP Connect**: إكمال المصافحة الثلاثية
- ✓ **SYN Scan**: إرسال حزم SYN دون إكمال المصافحة
- ✓ **UDP Scan**: فحص المنافذ المغلقة عبر رسائل ICMP
- ✓ **خصائص**: حجم النافذة، أنماط الحزم، التوقيت

No.	Time	Source	Destination	Protocol	Info
40	139.931107	Wistron_07:07:ee	broadcast	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=&ncp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

فلتر كشف TCP Connect

tcp.flags.syn == 1 and tcp.flags.ack == 0

فك تشفير جلسات SSL/TLS

- ✓ **Server Key**: استخدام مفتاح الخادم الخاص
- ✓ **SSLKEYLOGFILE**: متغير البيئة للمتصفحات
- ✓ **Pre-Master Secret**: تسجيل مفاتيح الجلسة
- ✓ **Decrypted Traffic**: عرض البيانات المشفرة

No.	Time	Source	Destination	Protocol	Info
7956	47.976502306	172.16.55.4	13.32.86.5	TCP	66 36790 → 443 [ACK] Seq=930
7957	47.976475071	13.32.86.5	172.16.55.4	TLSv1.3	90 Application Data
7958	47.977085523	172.16.55.4	13.32.86.5	TLSv1.3	90 Application Data
7959	47.977280665	172.16.55.4	13.32.86.5	TCP	66 36790 → 443 [FIN, ACK] Seq=930
7960	47.990649266	172.16.55.4	192.168.1.1	DNS	95 Standard query 0x68ad A t
7961	48.055524955	13.32.86.5	172.16.55.4	TCP	66 443 → 36790 [ACK] Seq=442
7962	48.055525028	13.32.86.5	172.16.55.4	TCP	66 443 → 36790 [ACK] Seq=442
7963	48.276824459	172.16.55.1	172.16.55.255	UDP	86 57621 → 57621 Len=44
7964	48.364671646	172.16.55.4	72.21.91.29	TCP	66 [TCP Dup ACK 77#4] 49384
7965	48.390217503	172.16.55.4	151.101.128.201	TLSv1.2	112 Application Data
7966	48.443683852	72.21.91.29	172.16.55.4	TCP	66 [TCP Dup ACK 78#4] [TCP A
7967	48.468658507	151.101.128.201	172.16.55.4	TCP	66 443 → 58838 [ACK] Seq=1 A
7968	48.745091062	151.101.128.201	172.16.55.4	TLSv1.2	112 Application Data
7969	48.745132245	172.16.55.4	151.101.128.201	TCP	66 58838 → 443 [ACK] Seq=47

إعداد Wireshark لفك التشفير

Edit → Preferences → Protocols → SSL → (Pre)-Master-Secret log filename

تحليل سلوك البرامج الضارة

- ✓ **Beaconing**: اتصالات منتظمة بخوادم التحكم
- ✓ **DNS Tunneling**: استخدام DNS لتعمير البيانات
- ✓ **Anomalous Traffic**: حركة مرور غير معتادة
- ✓ **Exfiltration**: تسريب البيانات

No.	Time	Source	Destination	Protocol	Info
6	0.07697	Auto Scroll in Live Capture		TCP	54 [TCP Dup ACK 2#1] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7	0.102939	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
8	0.102946	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 2#2] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9	0.128285	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
10	0.128319	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 2#3] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11	0.154162	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
12	0.154169	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 2#4] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179906	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
14	0.179915	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

فلتر كشف الاتصالات المنتظمة

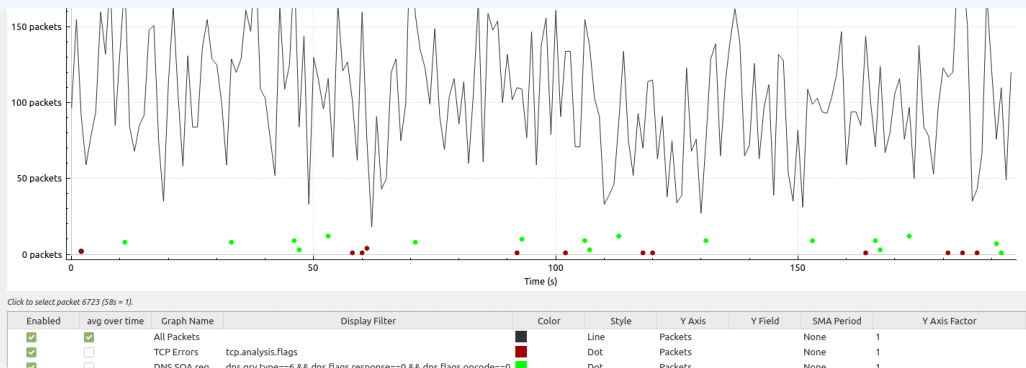
frame.time_delta > 10 && frame.time_delta < 60

التحليل البصري والرسوم البيانية

رسوم الحزم، رسوم I/O، خرائط GeoIP، وتصور هرميات البروتوكول

رسوم I/O لتحليل حركة المرور

- ✓ **رسوم بيانية:** تمثيل حركة المرور عبر الزمن
- ✓ **فلتر متقدمة:** تطبيق فلتر على الرسوم
- ✓ **مقارنة:** مقارنة بروتوكولات متعددة
- ✓ **تصدير:** حفظ الرسوم للتحليل

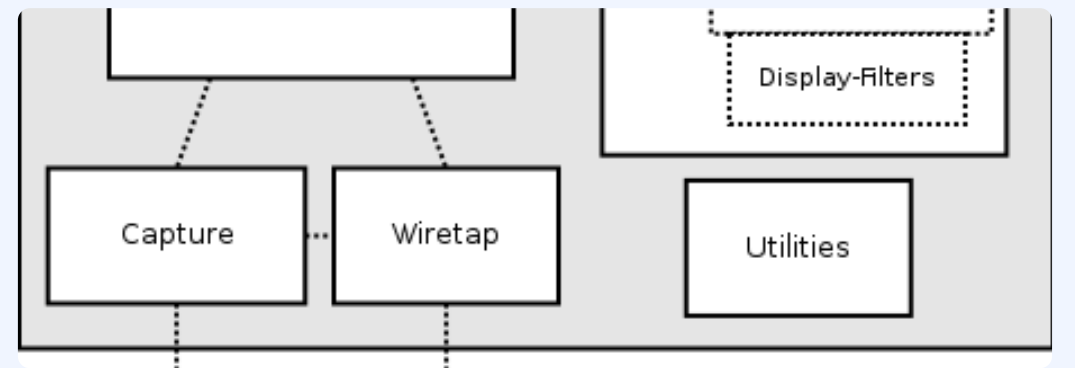


الوصول للميزة

Statistics → I/O Graph

رسوم الحزم (Packet Diagrams)

- ✓ **عرض مرئي:** تمثيل بصري للحزم والحقول
- ✓ **تفاعلي:** النقر على العناصر لتمييزها
- ✓ **عرض القيم:** إظهار قيم الحقول
- ✓ **فلتر:** عرض فلتر عند التمرير

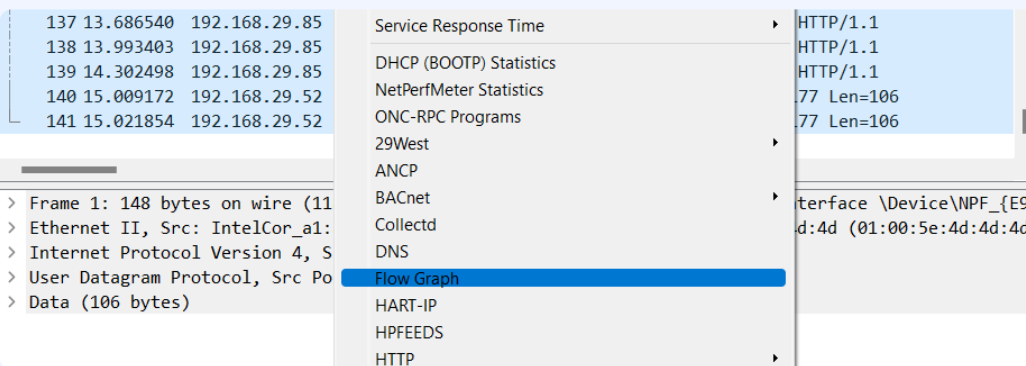


تفعيل الميزة

Edit → Preferences → Layout → Packet Diagram

تصور هرميات البروتوكول

- ✓ **هرم OSI:** عرض طبقات الشبكة
- ✓ **تسلسل:** عرض تسلسل البروتوكولات
- ✓ **تحليل:** تحليل العلاقات بين البروتوكولات
- ✓ **إحصائيات:** إحصائيات البروتوكولات

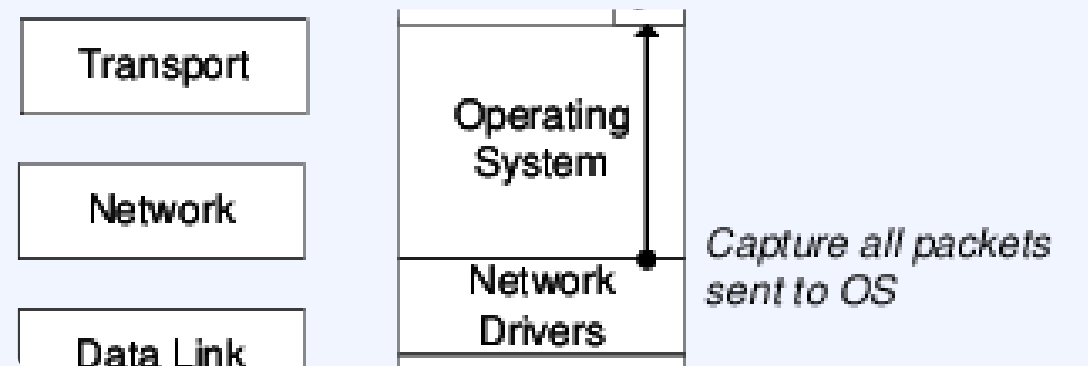


عرض إحصائيات البروتوكول

Statistics → Protocol Hierarchy

خرائط GeoIP

- ✓ **تحديد الموقع:** تحديد المواقع الجغرافية
- ✓ **فلتر:** فلتر حسب الدولة/المنطقة
- ✓ **ASN:** تحديد أرقام أنظمة المستقل
- ✓ **قواعد البيانات:** استخدام Maxmind GeoLite



فلتر حسب الموقع

ip and not ip.geoip.asnum == 63949

المهام والتمارين العملية

تمارين تحليل خطوة بخطوة، سيناريوهات واقعية، استكشاف أخطاء الشبكة، دراسات حالة للتحقيقات الأمنية

سيناريوهات واقعية

- بطء الشبكة: تحديد أسباب التأخير
- انقطاع الاتصال: تحليل فقدان الحزم
- تطبيقات بطيئة: تشخيص مشاكل التطبيقات
- ازدحام الشبكة: تحديد مصادر الازدحام

No.	Time	Source	Destination	Protocol	Length	Info
52	1.483938	10.2.12.1	224.0.0.5	OSPF	130	Hello Packet
53	1.515328	10.31.166.12	10.2.12.140	UDP	60	3389 → 58863 Len=60
54	2.189810	192.1.192.11	10.2.12.140	TLSv1.2	97	Application Data
55	2.230756	10.21.12.140	192.1.192.11	TCP	54	51990 → 852 [ACK] Seq=1 A

مهمة عملية

حلل ملف PCAP يحتوي على مشكلة بطء في التصفح وحدد السبب

تمارين تحليل خطوة بخطوة

- التقاط الحزم: تحديد واجهة الشبكة وتطبيق الفلاتر
- تحليل البروتوكول: فحص حزم TCP/UDP/HTTP
- متابعة التدفقات: استخدام Follow TCP Stream
- استخراج البيانات: تصدير الكائنات من الحزم

No.	Time	Source	Destination	Protocol	Info
49246	4.43	192.168.1.101	74.125.200.94	TCP	49246 → 443 [ACK] Seq=3161453776 Ack=1710850200 Win=4150 Len=0 TSval=595569056 TSecr=3513932058
49247	4.43	192.168.1.101	74.125.200.94	TLSv1.2	Application Data
443	4.9251	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=1298278402 Ack=1710850200 Win=371 Len=0 TSval=1704563776 TSecr=595569052
443	4.9246	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=3708602291 Ack=3161453776 Win=547 Len=0 TSval=3513932109 TSecr=595569029
443	4.9249	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=2905517011 Ack=521750204 Win=306 Len=0 TSval=1415548817 TSecr=595569030
443	4.9246	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=3708602291 Ack=3161453776 Win=547 Len=0 TSval=3513932161 TSecr=595569056
443	4.9251	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=1298278402 Ack=1710850200 Win=371 Len=0 TSval=1704563942 TSecr=595569042
443	4.9251	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=1030802300 Ack=360272818 Win=4096 Len=0 TSval=595570899 TSecr=3031662643
443	4.9251	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=1277483 Ack=1149722157 Win=7875 Len=0 TSval=212941084 TSecr=595572845
443	4.9251	192.168.1.101	192.168.1.101	TLSv1.2	Continuation Data
443	4.9251	192.168.1.101	192.168.1.101	TCP	443 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
443	4.9251	192.168.1.101	192.168.1.101	HTTP	HTTP Version 4, client
443	4.9251	192.168.1.101	192.168.1.101	HTTP	HTTP Version 4, server
443	4.9251	192.168.1.101	192.168.1.101	ICMPv6	Router Advertisement from 94:fb:b2:bd:df:d8

مهمة عملية

النظرة على حركة مرور HTTP وقم بتحليل الطلبات والردود باستخدام Follow TCP Stream

دراسات حالة للتحقيقات الأمنية

- هجوم MITM: تحليل هجمات الرجل في المنتصف
- برامج ضارة: كشف سلوك البرامج الخبيثة
- مسح الشبكة: تحديد عمليات المسح غير المصرح بها
- تسريب البيانات: تحليل محاولات استخراج البيانات

No.	Time	Source	Destination	Protocol	Length	Info
6	0.076978	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#1] [TCP ACKed unseen seg.4] [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7	0.102939	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
8	0.102946	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#2] [TCP ACKed unseen seg.4] [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9	0.128285	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
10	0.128319	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#3] [TCP ACKed unseen seg.4] [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11	0.154162	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
12	0.154169	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#4] [TCP ACKed unseen seg.4] [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179906	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
14	0.179915	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

مهمة عملية

حلل ملف PCAP يحتوي على هجوم ARP Poisoning وحدد الجهاز المهاجم

استكشاف أخطاء الشبكة

- مشاكل DNS: تحليل استعلامات DNS
- مشاكل DHCP: تتبع عملية تخصيص العناوين
- إعادة الإرسال: تحليل TCP Retransmission
- مشاكل ARP: كشف تضارب عناوين MAC

No.	Time	Source	Destination	Protocol	Length	Info
13	5.711243	192.168.29.52	54.227.131.71	TCP	55	52531 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
32	13.122433	192.168.29.52	18.155.107.101	TCP	55	52527 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
50	20.410580	192.168.29.52	54.227.131.71	TCP	54	52532 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
52	20.410926	192.168.29.52	54.227.131.71	TCP	54	52532 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
55	20.434244	192.168.29.52	54.227.131.71	TCP	54	52531 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
56	20.434881	192.168.29.52	54.227.131.71	TCP	54	52531 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
61	22.730248	192.168.29.52	35.83.172.235	TCP	55	52534 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
62	22.888390	192.168.29.52	35.83.172.235	TCP	55	52533 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
65	23.679332	192.168.29.52	35.83.172.235	TCP	55	52536 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
66	23.757407	192.168.29.52	35.83.172.235	TCP	55	52535 → 443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
93	36.636903	192.168.29.52	35.83.172.235	TLSv1.2	131	Ignored

مهمة عملية

استخدم Wireshark لتشخيص مشكلة في اتصال جهاز بالشبكة

قضية عملية 1: تحليل أداء الشبكة

تحديد أسباب بطء الشبكة وتحليل زمن الاستجابة وتحديد نقاط الازدحام

الأدوات والفلاتر المستخدمة

فلتر زمن الاستجابة

frame.time_delta > 0.1

فلتر إعادة الإرسال

tcp.analysis.retransmission

فلتر فقدان الحزم

tcp.analysis.lost_segment

أداة إحصائيات نقطة النهاية

Statistics → Endpoints → IPv4

أداة رسوم I/O

Statistics → I/O Graph

خطوات التحليل

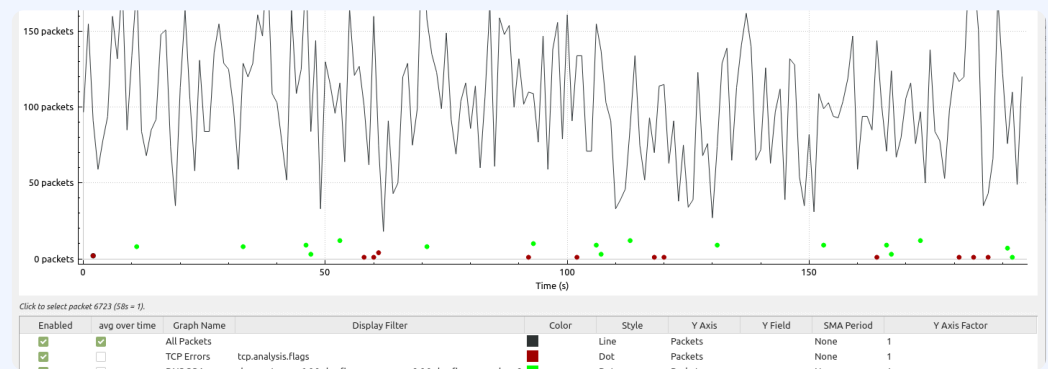
التقاط البيانات: بدء التقاط حركة المرور على الواجهة المعنية

تطبيق الفلاتر: استخدام فلتر لعزل حركة المرور ذات الصلة

تحليل I/O Graph: مراقبة أنماط حركة المرور عبر الزمن

فحص الحزم: تحليل الحزم ذات زمن الاستجابة المرتفع

تحديد المشاكل: البحث عن إعادة الإرسال وفقدان الحزم



مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة يحتوي على مشكلة أداء

تحليل الحزم: استخدم الفلاتر لتحديد الحزم ذات المشاكل

إنشاء رسوم بيانية: استخدم I/O Graph لتمثيل حركة المرور

تقرير النتائج: قم بإعداد تقرير يلخص النتائج والتوصيات

No.	Time	Source	Destination	Protocol	Info
40	139.931167	Wistron_07:07:ee	Broadcast	ARP	who has 192.168.1.254? tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	192.168.1.68	66.102.9.99	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.219216	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

النتائج والتوصيات

تحديد نقاط الازدحام: تحديد الأجهزة أو الروابط المسببة للازدحام

تحليل زمن الاستجابة: حساب متوسط زمن الاستجابة للشبكة

تحديد الأسباب: تحديد ما إذا كان البطء بسبب الأجهزة أو البرمجيات

توصيات التحسين: اقتراح حلول لتحسين أداء الشبكة

مستوى إكمال التحليل: 75%

قضية عملية 2: كشف هجمات الشبكة

استخدام Wireshark للكشف عن هجمات DDoS ومحاولات الاختراق وأنماط الحركة المشبوهة

فلاتر الكشف عن الهجمات

كشف هجمات DDoS ⚡

```
ip.src==192.168.1.1 && frame.time_delta < 0.01
```

كشف عمليات المسح 🔍

```
tcp.flags.syn==1 && tcp.flags.ack==0
```

كشف محاولات الدخول الفاشلة ❗

```
ftp.response.code == 530 ||  
ssh.connection.auth_failure
```

كشف هجمات ARP Spoofing 🏠

```
arp.duplicate-address-detected
```

كشف أنشطة البرامج الضارة ⚡

```
"dns.qry.name matches "(malicious|suspicious)"
```

أنواع الهجمات المشتركة

Port Scanning 🚩

Man-in-the-Middle 🏠

DDoS 🏠

SQL Injection ⚠️

Malware ⚡

Brute Force 🔒

هجمات DDoS: فيضان الحزم من مصادر متعددة 🏠

MITM: اعتراض وتعديل البيانات أثناء النقل 🏠

Port Scanning: فحص المنافذ المفتوحة بحثاً عن ثغرات 🔍

Brute Force: محاولات دخول متكررة بكلمات مرور مختلفة 🔒

No.	Time	Source	Destination	Protocol	Info
40	139.93110	Wistron_07:07:ee	Broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=&cp=1 HTTP/1.1
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.219210	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة يحتوي على هجوم

تحليل الحزم: استخدم الفلاتر لتحديد نوع الهجوم 🔍

إنشاء رسوم بيانية: استخدم I/O Graph لتحليل نمط الهجوم 📊

تقرير النتائج: قم بإعداد تقرير يحدد نوع الهجوم ومصدره 📄

No.	Time	Source	Destination	Protocol	Info
3775	59.181975587	HonHaiPr_58:51:f9	44:59:43:4c:49:04	ARP	42 192.168.10.2 is at 9c:d2:1e:58:51:f9

Frame 3034: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: 44:59:43:4c:49:04 (44:59:43:4c:49:04), Dst: HonHaiPr_58:51:f9 (9c:d2:1e:58:51:f9)
Destination: HonHaiPr_58:51:f9 (9c:d2:1e:58:51:f9)
Source: 44:59:43:4c:49:04 (44:59:43:4c:49:04)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 44:59:43:4c:49:04 (44:59:43:4c:49:04)
Sender IP address: 192.168.10.1
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.10.2

تحليل أنماط الهجمات

رسوم I/O: تحديد زيادة غير طبيعية في حركة المرور 📊

GeoIP: تحديد مصادر الهجمات الجغرافية 🌐

تحليل التوقيت: تحديد أنماط تكرار الهجمات 🕒

تحليل البروتوكول: تحديد البروتوكولات المستهدفة 🏠

مستوى إكمال التحليل: 65%

No.	Time	Source	Destination	Protocol	Info
6	0.07697	200.121.1.131	172.16.0.122	TCP	54 [TCP Dup ACK 281] [TCP ACKed unseen seg-4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7	0.102939	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
8	0.102946	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 282] [TCP ACKed unseen seg-4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9	0.128285	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
10	0.128319	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 283] [TCP ACKed unseen seg-4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11	0.154162	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
12	0.154169	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 284] [TCP ACKed unseen seg-4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179906	200.121.1.131	172.16.0.122	TCP	1454 [TCP segment of a reassembled PDU]
14	0.179915	172.16.0.122	200.121.1.131	TCP	54 [TCP Dup ACK 285] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400

قضية عملية 3: تحليل بروتوكولات الشبكة

دراسة متعمقة لبروتوكولات TCP/IP و HTTP/DNS وتحليل سلوكها في ظروف مختلفة

فلاتر تحليل البروتوكولات

تحليل مصافحة TCP

```
tcp.flags.syn == 1 || tcp.flags.ack == 1
```

كشف إعادة إرسال TCP

```
tcp.analysis.retransmission
```

تحليل طلبات HTTP

```
"http.request.method == "GET
```

تحليل استعلامات DNS

```
dns.qry.type == 1 && dns.flags.response == 0
```

كشف أخطاء البروتوكول

```
tcp.analysis.flags || icmp.type == 3
```

بروتوكولات الشبكة الرئيسية

TLS ARP ICMP UDP DNS HTTP IP TCP

TCP: بروتوكول التحكم في الإرسال - موثوقية وموجه الاتصال

IP: بروتوكول الإنترنت - توجيه الحزم وعنونة الشبكة

HTTP: بروتوكول نقل النص التشعبي - طلبات واستجابات الويب

DNS: نظام أسماء النطاقات - ترجمة النطاقات إلى عناوين IP

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of a selected packet (No. 349), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response) sections.

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة

تطبيق الفلاتر: استخدم فلاتر البروتوكولات

تحليل الأداء: قارن أداء البروتوكولات المختلفة

تقرير النتائج: قم بإعداد تقرير بتحليل البروتوكولات

The screenshot shows a detailed view of a packet in Wireshark. The top pane displays the packet list, and the bottom pane shows the details of a selected packet (No. 23), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data sections.

تحليل سلوك البروتوكولات

زمن الاستجابة: قياس زمن استجابة DNS و HTTP

الضغط: تحليل استخدام ضغط HTTP

التشفير: تحليل اتصالات TLS/SSL

الأداء: مقارنة أداء TCP مقابل UDP

مستوى إكمال التحليل: 80%

The screenshot shows a detailed view of a packet in Wireshark. The top pane displays the packet list, and the bottom pane shows the details of a selected packet (No. 7), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data sections.

قضية عملية 4: استكشاف أخطاء الاتصال وتشخيصها

استخدام Wireshark لتشخيص مشاكل الاتصال وفقدان الحزم وإعادة الإرسال

فلاتر تشخيص المشاكل

كشف إعادة الإرسال

tcp.analysis.retransmission

كشف فقدان الحزم

tcp.analysis.lost_segment

كشف التأخير

frame.time_delta > 0.1

كشف أخطاء TCP

tcp.analysis.flags

كشف الازدحام

tcp.window_size < 1000

أنواع مشاكل الاتصال الشائعة

انقطاع الاتصال

تأخير الاستجابة

إعادة الإرسال

فقدان الحزم

ازدحام الشبكة

فقدان الحزم: حزم تصل متأخرة أو لا تصل على الإطلاق

إعادة الإرسال: إرسال نفس الحزمة مرة أخرى

تأخير الاستجابة: زمن استجابة أعلى من الطبيعي

انقطاع الاتصال: انقطاع مفاجئ في الاتصال

No.	Time	Source	Destination	Protocol	Length	Info
13	5.711243	192.168.29.52	54.227.131.71	TCP	55	52531
32	13.122433	192.168.29.52	18.155.107.101	TCP	55	52527
50	20.410580	192.168.29.52	54.227.131.71	TCP	54	52532
52	20.410926	192.168.29.52	54.227.131.71	TCP	54	52532
55	20.434244	192.168.29.52	54.227.131.71	TCP	54	52531
56	20.434881	192.168.29.52	54.227.131.71	TCP	54	52531
61	22.730248	192.168.29.52	35.83.172.235	TCP	55	52534
62	22.888390	192.168.29.52	35.83.172.235	TCP	55	52533
65	23.679332	192.168.29.52	35.83.172.235	TCP	55	52536
66	23.757407	192.168.29.52	35.83.172.235	TCP	55	52535
93	36.636903	192.168.29.52	35.83.172.235	TLSv1.2	131	Ignored

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة به مشاكل

تشخيص المشاكل: استخدم الفلاتر لكشف المشاكل

تحليل الأداء: استخدم الأدوات لتحليل الأداء

تقرير النتائج: قم بإعداد تقرير بالتشخيص والحلول

No.	Time	Source	Destination	Protocol	Length	Info
52	1.483938	10.2.12.1	224.0.0.5	OSPF	130	Hello Packet
53	1.515328	10.31.166.12	10.2.12.140	UDP	60	3389 → 58863 Len=60
54	2.189810	192.1.192.11	10.2.12.140	TLSv1.2	97	Application Data
55	2.230756	10.21.12.140	192.1.192.11	TCP	54	51990 → 852 [ACK] Seq=1 A

أدوات التشخيص المتقدمة

رسوم I/O: تحليل أنماط حركة المرور

متابعة التدفق: تحليل اتصالات TCP كاملة

إحصائيات نقطة النهاية: تحديد الأجهزة النشطة

معلومات الخبير: تحديد المشاكل المحتملة

مستوى إكمال التشخيص: 70%

No.	Time	Source	Destination	Protocol	Length	Info
622	58.596644	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
623	58.597421	172.217.166.206	192.168.43.236	TCP	54	443 → 37699 [RST] Seq=41 Win=0 Len=0
624	58.597889	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
625	58.598037	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
626	59.731513	192.168.43.236	172.217.166.232	TLSv1.2	93	Application Data
627	59.731863	192.168.43.236	172.217.166.232	TCP	54	1160 → 443 [FIN, ACK] Seq=103 Ack=40 Win=67 Len=0
628	59.732085	192.168.43.236	172.217.166.232	TCP	54	1160 → 443 [FIN, ACK] Seq=103 Ack=40 Win=67 Len=0
629	60.623397	172.217.166.232	192.168.43.236	TCP	60	[TCP Dup ACK (64)] Seq=1160 Ack=40 Win=240 Len=0 SLE=103 SRC=104
630	60.625580	172.217.166.232	192.168.43.236	TCP	54	443 → 1160 [FIN, ACK] Seq=40 Ack=104 Win=240 Len=0
631	60.626840	192.168.43.236	172.217.166.232	TCP	54	1160 → 443 [ACK] Seq=104 Ack=41 Win=67 Len=0

قضية عملية 5: تحليل حركة المرور المشفرة

تقنيات فك تشفير TLS/SSL وتحليل حركة المرور المشفرة باستخدام Wireshark

تقنيات فك التشفير

استخدام مفتاح الخادم الخاص

Edit → Preferences → Protocols → SSL → RSA Keys list

ملف سجل مفاتيح الجلسة

SSLKEYLOGFILE=~/.sslkeylogfile.log

إعداد Wireshark لفك التشفير

Edit → Preferences → Protocols → SSL → (Pre)-Master-Secret log filename

فلتر حركة المرور المشفرة

ssl || tls

متابعة تدفق SSL

Analyze → Follow → SSL Stream

بروتوكولات التشفير الشائعة

SSH FTPS HTTPS SSL 3.0 TLS 1.2 TLS 1.3

TLS/SSL: بروتوكولات تأمين طبقة النقل

المفاتيح: مفاتيح متناظرة وغير متناظرة

الشهادات: شهادات X.509 للتحقق من الهوية

مصافحة TLS: عملية التفاوض على خوارزمية التشفير

No.	Time	Source	Destination	Protocol	Length	Info
7956	47.976502306	172.16.55.4	13.32.86.5	TCP	66	36790 → 443 [ACK] Seq=930
7957	47.976475071	13.32.86.5	172.16.55.4	TLSv1.3	90	Application Data
7958	47.977085523	172.16.55.4	13.32.86.5	TLSv1.3	90	Application Data
7959	47.977280665	172.16.55.4	13.32.86.5	TCP	66	36790 → 443 [FIN, ACK] Seq=930
7960	47.990649266	172.16.55.4	192.168.1.1	DNS	95	Standard query 0x68ad A t
7961	48.055524955	13.32.86.5	172.16.55.4	TCP	66	443 → 36790 [ACK] Seq=442
7962	48.055525028	13.32.86.5	172.16.55.4	TCP	66	443 → 36790 [ACK] Seq=442
7963	48.276824459	172.16.55.1	172.16.55.255	UDP	86	57621 → 57621 Len=44
7964	48.364671646	172.16.55.4	72.21.91.29	TCP	66	[TCP Dup ACK 77#4] 49384
7965	48.390217503	172.16.55.4	151.101.128.201	TLSv1.2	112	Application Data
7966	48.443683852	72.21.91.29	172.16.55.4	TCP	66	[TCP Dup ACK 78#4] [TCP A
7967	48.468658507	151.101.128.201	172.16.55.4	TCP	66	443 → 58838 [ACK] Seq=1 A
7968	48.745091062	151.101.128.201	172.16.55.4	TLSv1.2	112	Application Data
7969	48.745132245	172.16.55.4	151.101.128.201	TCP	66	58838 → 443 [ACK] Seq=47

Internet Protocol Version 4, Src: 13.35.105.92, Dst: 172.16.55.4
Transmission Control Protocol, Src Port: 443, Dst Port: 44428, Seq: 1, Ack: 1, Len: 2628
Transport Layer Security

مهمة عملية

إعداد البيئة: تكوين متغير البيئة SSLKEYLOGFILE

إعداد Wireshark: تكوين Wireshark لاستخدام ملف السجل

التقاط الجلسات: التقاط حركة مرور HTTPS

تحليل النتائج: تحليل البيانات بعد فك التشفير

No.	Time	Source	Destination	Protocol	Length	Info	
3	0.000001	0.000000	ec2-44-226-235-245...	192.168.0.169	TCP	66	0 0xd
4	0.000002	0.000000	ec2-44-226-235-245...	192.168.0.169	TLSv1...	382	316 0xd
5	0.000002	0.000000	ec2-44-226-235-245...	192.168.0.169	TLSv1...	104	38 0xd
6	0.000342	0.000340	192.168.0.169	ec2-44-226-235-245...	TCP	66	0 0x0
7	0.059744	0.059402	ec2-44-226-235-245...	192.168.0.169	TCP	1474	1408 0xd
8	0.060013	0.000269	192.168.0.169	ec2-44-226-235-245...	TCP	66	0 0x0
9	0.061261	0.001248	ec2-44-226-235-245...	192.168.0.169	TCP	1474	1408 0xd
10	0.061263	0.000002	ec2-44-226-235-245...	192.168.0.169	TCP	1474	1408 0xd
11	0.061264	0.000001	ec2-44-226-235-245...	192.168.0.169	TCP	1474	1408 0xd

خطوات تحليل التشفير

إعداد البيئة: تكوين متغير البيئة SSLKEYLOGFILE

إعادة تشغيل المتصفح: إعادة تشغيل المتصفح بعد الإعداد

بدء الالتقاط: بدء التقاط الحزم في Wireshark

تحليل الجلسات: عرض البيانات بعد فك التشفير

مستوى إكمال التحليل: 85%

No.	Time	Source	Destination	Protocol	Length	Info
15	5.637437	192.168.29.52	54.200.149.178	TLSv1.2	5784	Application Data
16	5.995543	54.200.149.178	192.168.29.52	TLSv1.2	5784	Application Data
17	5.995543	54.200.149.178	192.168.29.52	TCP	443	→ 5784 [ACK] Seq=1 Ack=75 Win=773 ...
18	5.995543	54.200.149.178	192.168.29.52	TCP	443	→ 5784 [ACK] Seq=1 Ack=180 Win=773 ...
19	5.995543	54.200.149.178	192.168.29.52	TLSv1.2	5784	Application Data
20	5.995543	54.200.149.178	192.168.29.52	TLSv1.2	5784	Application Data
21	5.995695	192.168.29.52	54.200.149.178	TCP	5784	→ 443 [ACK] Seq=180 Ack=401 Win=2 ...
22	5.997280	192.168.29.52	224.77.77.77	TLSv1.2	5784	Application Data
23	6.013406	192.168.29.52	224.77.77.77	UDP	12177	→ 12177 Len=106
6.024880	12177	12177	12177	UDP	12177	→ 12177 Len=106
6.324210	58033	58033	58033	TCP	58033	→ 443 [ACK] Seq=1 Ack=1 Win=813 L...
6.327225	5784	5784	5784	TCP	443	→ 5784 [ACK] Seq=401 Ack=222 Win=7...
6.349476	58033	58033	58033	TCP	443	→ 58033 [ACK] Seq=1 Ack=2 Win=295 L...
6.404258	58033	58033	58033	ARP	150	has 150.168.28.1837 Tel 150.168.28.1...
6.497651	58033	58033	58033	TCP	58033	→ 443 [ACK] Seq=1 Ack=1 Win=813 L...
6.550675	58033	58033	58033	TCP	443	→ 58033 [ACK] Seq=1 Ack=2 Win=813 L...
6.750657	58033	58033	58033	TCP	58033	→ 443 [ACK] Seq=1 Ack=1 Win=813 L...
6.786480	58033	58033	58033	TCP	443	→ 58033 [ACK] Seq=1 Ack=2 Win=133 L...

قضية عملية 6: تحليل سلوك التطبيقات

استخدام Wireshark لتحليل حركة مرور التطبيقات وتحديد مشاكل الأداء والأخطاء

فلاتر تحليل التطبيقات

تحليل حركة مرور HTTP

```
http.request.method == "GET" ||  
"http.request.method == "POST"
```

تحليل استعلامات قاعدة البيانات

```
mysql || postgres || tds
```

تحليل البريد الإلكتروني

```
smtp || pop || imap
```

تحليل نقل الملفات

```
ftp || sftp || smb
```

تحليل أداء التطبيق

```
tcp.time_delta > 0.1
```

أنواع التطبيقات المشتركة

تطبيقات الويب قواعد البيانات البريد الإلكتروني نقل الملفات

الدرشة بث الفيديو

تطبيقات الويب: HTTP/HTTPS, REST APIs

قواعد البيانات: MySQL, PostgreSQL, MongoDB

البريد الإلكتروني: SMTP, POP3, IMAP

نقل الملفات: FTP, SFTP, SMB

No.	Time	Source	Destination	Protocol	Info
47	139.931463	ThomsonT_08:35:4f	192.168.1.254	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة

تطبيق الفلاتر: استخدم فلاتر التطبيقات

تحليل الأداء: قسّم زمن استجابة التطبيق

تقرير النتائج: قم بإعداد تقرير بتحليل التطبيق

No.	Time	Source	Destination	Protocol	Length	Info
52	1.483938	10.2.12.1	224.0.0.5	OSPF	130	Hello Packet
53	1.515328	10.31.166.12	10.2.12.140	UDP	60	3389 → 58863 Len=
54	2.189810	192.1.192.11	10.2.12.140	TLSv1.2	97	Application Data
55	2.230756	10.21.12.140	192.1.192.11	TCP	54	51990 → 852 [ACK] Seq=1 A

تحليل مشاكل الأداء

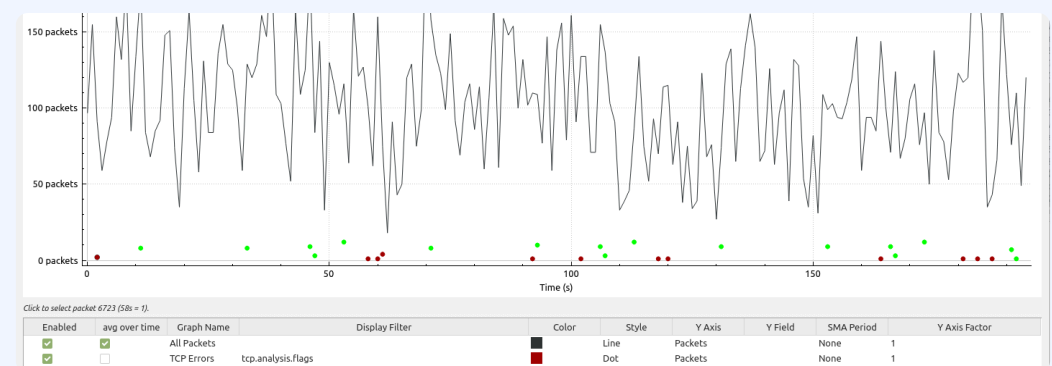
زمن الاستجابة: قياس زمن استجابة التطبيق

الأخطاء: تحديد أخطاء التطبيق والشبكة

الضغط: تحليل استخدام ضغط البيانات

الاتصالات: تحليل عدد الاتصالات المتزامنة

مستوى إكمال التحليل: 75%



قضية عملية 7: تحليل الشبكات اللاسلكية

استخدام Wireshark لتحليل حركة مرور الشبكات اللاسلكية وكشف نقاط الضعف الأمنية

فلاتر تحليل الشبكات اللاسلكية

فلاتر حزم 802.11

wlan

فلاتر حزم WPA/WPA2

wlan.wpa || wlan.rsn

فلاتر نقاط الوصول

wlan.fc.type_subtype == 0x08

فلاتر هجمات Deauthentication

wlan.fc.type_subtype == 0x0c

فلاتر إشارات الاكتشاف

wlan.fc.type_subtype == 0x04

بروتوكولات الشبكات اللاسلكية

WPS

WPA3

WPA2

WPA

WEP

802.11

802.11: معايير الشبكات اللاسلكية

بروتوكولات التشفير: WEP, WPA, WPA2, WPA3

WPS: إعداد Wi-Fi المحمي

أنواع الحزم: إطارات التحكم، البيانات، الإدارة

The screenshot shows a list of network packets in Wireshark. The selected packet is a TCP window update (Seq=17760, Ack=909667, Len=0) from 192.168.0.5 to 198.35.26.96. Below the list, the packet details pane shows the Ethernet II header (Src: 44:59:43:4c:49:04, Dst: CloudNet_9f:41:11) and the Internet Protocol Version 4 header (Src: 198.35.26.96, Dst: 192.168.0.5).

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة لاسلكية

تطبيق الفلاتر: استخدم فلاتر الشبكات اللاسلكية

كشف الثغرات: حدد نقاط الضعف الأمنية

تقرير النتائج: قم بإعداد تقرير بالتحليل والتوصيات

كشف نقاط الضعف الأمنية

شبكات مفتوحة: كشف الشبكات غير المشفرة

هجمات Evil Twin: كشف نقاط وصول مزيفة

هجمات Deauth: كشف محاولات قطع الاتصال

ثغرات WPS: كشف نقاط الضعف في WPS

مستوى إكمال التحليل: 80%

The screenshot shows a list of network packets in Wireshark. The selected packet is a TCP segment of a reassembled PDU (Seq=1, Ack=11201, Win=63000, Len=0) from 192.168.0.122 to 200.121.1.131. Below the list, the packet details pane shows the Ethernet II header (Src: Vmware_c0:00:01, Dst: Vmware_42:12:13) and the Internet Protocol Version 4 header (Src: 200.121.1.131, Dst: 172.16.0.122).

The screenshot shows a list of network packets in Wireshark. The selected packet is an ARP request (Type: ARP, 0x0806) from 44:59:43:4c:49:04 to 00:00:00:00:00:00. Below the list, the packet details pane shows the Ethernet II header (Hardware type: Ethernet, Protocol type: IPv4) and the Internet Protocol Version 4 header (Source MAC address: 44:59:43:4c:49:04, Target MAC address: 00:00:00:00:00:00).

قضية عملية 8: تحليل حركة المرور الصوتية والفيديو (VoIP)

استخدام Wireshark لتحليل حركة مرور VoIP وتحديد مشاكل الجودة والأداء

فلاتر تحليل VoIP

فلتر حزم SIP

sip

فلتر حزم RTP

rtp

فلتر حزم RTCP

rtcp

فلتر مكالمات SIP

"sip.Method == "INVITE"

فلتر مشاكل RTP

rtp.ssrc || rtp.seq || rtp.timestamp

بروتوكولات VoIP الرئيسية

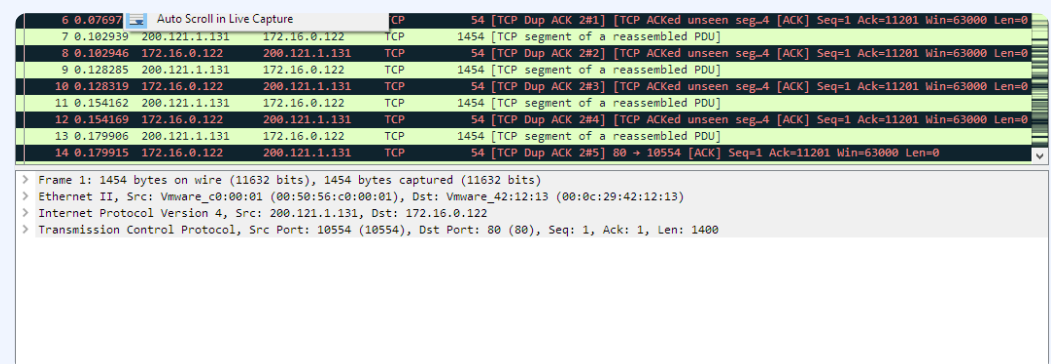
Skinny MGCP H.323 RTCP RTP SIP

SIP: بروتوكول بدء الجلسة - إدارة المكالمات

RTP: بروتوكول النقل في الوقت الفعلي - نقل الصوت/الفيديو

RTCP: بروتوكول التحكم في RTP - مراقبة الجودة

H.323: مجموعة بروتوكولات للمؤتمرات الصوتية والمرئية



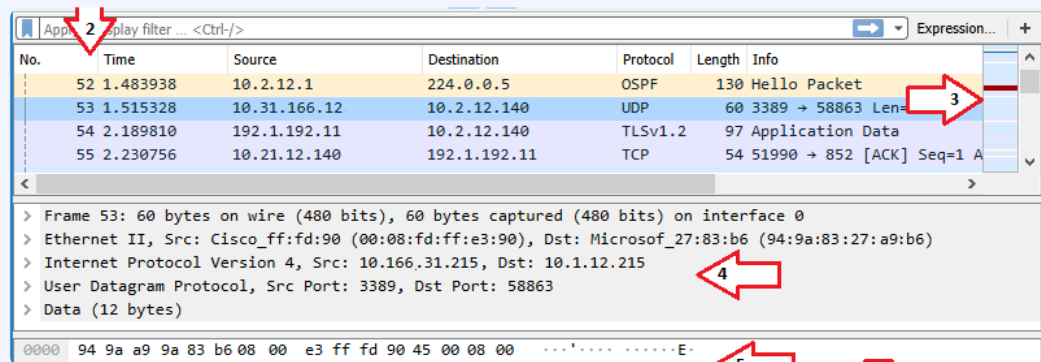
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط VoIP

تطبيق الفلاتر: استخدم فلاتر SIP و RTP

تحليل الجودة: استخدم أدوات تحليل RTP

تقرير النتائج: قم بإعداد تقرير بجودة الاتصال



تحليل جودة VoIP

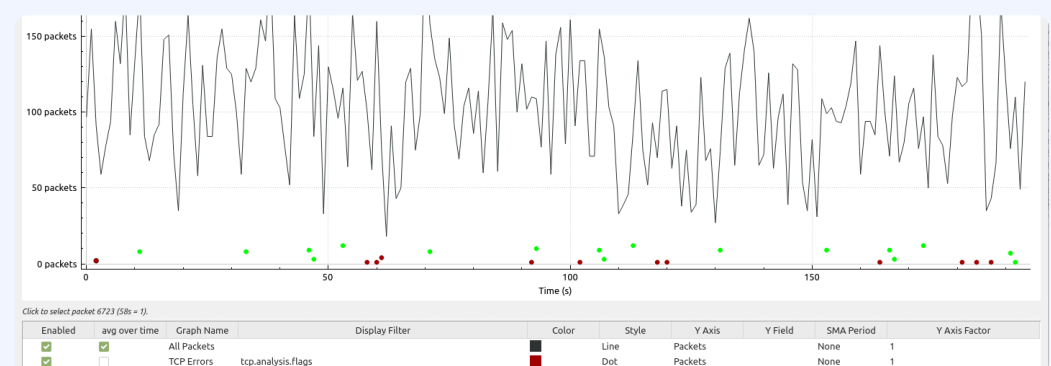
MOS: متوسط رأي المستخدم - قياس جودة الصوت

زمن الاستجابة: قياس التأخير في نقل الصوت

الاهتزاز: قياس تباين زمن الوصول للحزم

% فقدان الحزم: حساب نسبة الحزم المفقودة

مستوى إكمال التحليل: 75%



قضية عملية 9: استخراج البيانات والملفات من حزم الشبكة

استخدام Wireshark لاستخراج الملفات والبيانات من حزم الشبكة وتحليلها

أدوات استخراج الملفات

استخراج كائنات HTTP

...File → Export Objects → HTTP

استخراج ملفات SMB

...File → Export Objects → SMB

استخراج مرفقات البريد

...File → Export Objects → IMAP

فلتر الملفات المستخرجة

"http.content_type contains "image"

استخراج البيانات الثنائية

...File → Export Packet Dissections → As CSV

أنواع الملفات القابلة للاستخراج

أرشيف

ملفات وسائط

ملفات تنفيذية

مستندات

صور

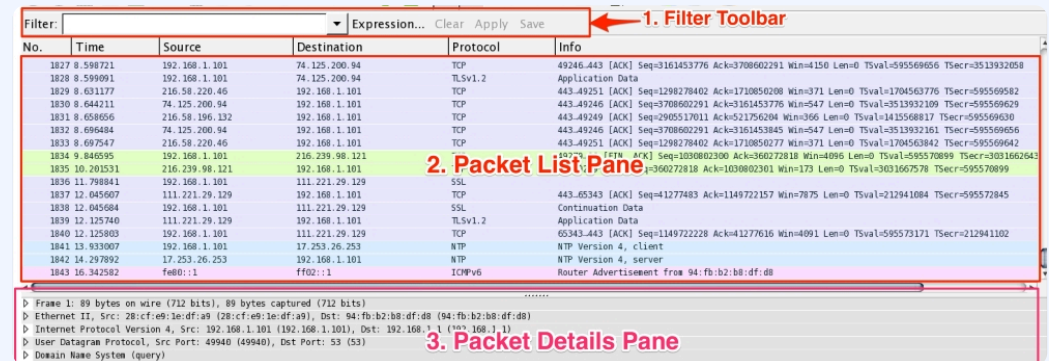
ملفات ضارة

الصور: JPEG, PNG, GIF, SVG

المستندات: PDF, DOCX, XLSX, PPTX

الملفات التنفيذية: EXE, DLL, APK

الأرشيف: ZIP, RAR, TAR, 7z



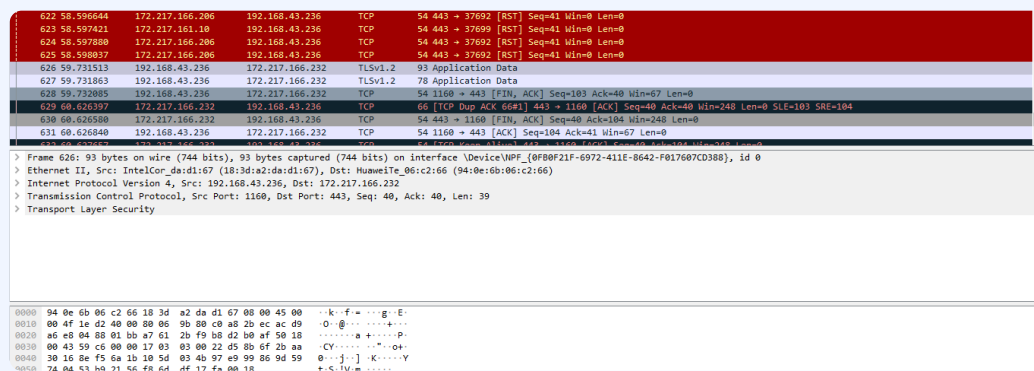
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة

تطبيق الفلاتر: استخدم فلتر لتحديد الملفات

استخراج الملفات: استخدم أدوات الاستخراج

تحليل النتائج: قم بتحليل الملفات المستخرجة



تقنيات تحليل الملفات المستخرجة

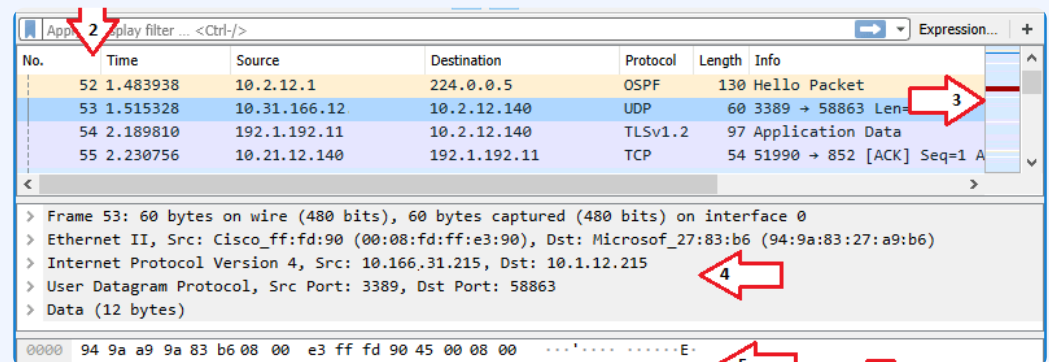
التحقق من سلامة الملف: حساب تجزئة MD5/SHA

كشف البرامج الضارة: فحص الملفات باستخدام مكافحة الفيروسات

التحليل الثنائي: فحص محتوى الملفات الثنائية

تحليل البيانات الوصفية: استخراج معلومات التعريف

مستوى إكمال التحليل: 85%



قضية عملية 10: تحقيق أمني متقدم

استخدام Wireshark في التحقيقات الأمنية المتقدمة وكشف التهديدات المعقدة وتحليل الهجمات المستمرة

فلاتر التحقيق الأمني

كشف حركة المرور المشبوهة

```
frame.time_delta < 0.01 && frame.len > 1000
```

كشف محاولات الاتصال المشبوهة

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

كشف أنشطة البرامج الضارة

```
"dns.qry.name matches "(malicious|suspicious)"
```

كشف تسريب البيانات

```
http contains "password" || http contains  
"credit_card"
```

كشف الاتصالات غير المعتادة

```
ip.dst == 0.0.0.0/0 && tcp.port > 10000
```

أنواع التهديدات الأمنية المتقدمة

اختراق البيانات هجمات التصيد برامج فدية هجمات صفرية APT

هجمات DDoS

APT: التهديدات المستمرة المتقدمة

هجمات صفرية: استغلال ثغرات غير معروفة

برامج فدية: تشفير الملفات وطلب فدية

هجمات التصيد: انتحال هوية موثوقة

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets, including several TCP segments (Seq=1, Ack=11201, Win=63000) and a frame (Frame 1) with details. The details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The frame length is 1454 bytes.

مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة بهجوم معقد

تطبيق الفلاتر: استخدم فلاتر التحقيق الأمني

تحليل الهجوم: حدد نوع الهجوم وأساليبه

تقرير التحقيق: قم بإعداد تقرير تحقيق أمني شامل

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets, including ARP, DNS, and HTTP traffic. The details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (request). The frame length is 42 bytes.

تقنيات التحليل المتقدمة

تحليل السلوك: تحديد أنماط السلوك غير المعتادة

تحليل الارتباطات: ربط الأحداث المختلفة معاً

تحليل البصمات: تحديد بصمات الهجمات المعروفة

التحليل الزمني: تحليل تسلسل الأحداث الزمني

مستوى إكمال التحقيق: 90%

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets, including an ARP request. The details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (request). The frame length is 42 bytes.