Oliver Krauss

Event Analysis

IS3523-001

9/21/2025

Executive Summary

This report presents a comprehensive analysis of a network packet capture from a 2005-era home environment, with the primary goal of determining whether malicious activity occurred during the monitored session. The capture was 8 minutes and 25 seconds long, with 2449 packets captured, totaling 811,157 bytes. Protocols observed included TCP, UDP, FTP, HTTP, ARP, DNS, legacy SSL variants, and the proprietary TiVoConnect protocol. The analysis focused on several indicators of compromise, including repeated anonymous FTP access, abnormal HTTP activity to sensitive sites, and the transfer of potentially unsafe executable and multimedia objects. By reconstructing the network timeline, the investigation indicated lateral movement, access to financial and academic accounts, and activity mirroring attack techniques now codified in frameworks such as MITRE ATT&CK. The client, who only used the computer for e-mail access through their Internet Service Provider (ISP), suspected intrusion. Evidence from the capture shows exploitation of a zero-day FTP vulnerability (CVE-2002-1345), multi-stage reconnaissance, likely exfiltration, and exposure to legacy malware delivery channels (e.g. SWF/Flash). While no malware transfers or credential theft was recorded, the assessment concludes that clear compromise and unauthorized data access occurred. Findings also emphasize how weaknesses in remote access and authentication could be leveraged for unauthorized information gathering and possible data theft, even by unsophisticated attackers in a home environment. Collectively, these actions formed a multi-stage attack chain: external compromise, lateral movement, privilege escalation, and probable data exfiltration (see Timeline and Fig. 6–15).

Methodology

The investigation followed best practices as outlined by NIST and SANS. The primary tools leveraged in this analysis were Wireshark and NetworkMiner, together with open-source intelligence. The process combined automated analysis and manual review to uncover the sequence of events, identify potential exploitation, and correlate traffic patterns with known attack vectors. Wireshark was the primary protocol analyzer to visualize packet flow, filter traffic by protocol, and reconstruct sessions. Key Wireshark features included display filters (e.g., ftp, dns, tcp.stream eq x, http), stream reconstruction, and timeline and volume analysis. NetworkMiner provided supplemental analysis for endpoint enumeration (hostnames, OS, Ips), file carving, and OS/protocol correlation. Automated I/O graphing and manual stream-follow analyses revealed periods of anomalous protocol behavior, which were afterwards mapped to attack stages using packet numbers and extracted endpoint evidence. Baseline environmental details and suspicious session initiation windows were reconstructed from DHCP, ARP, and endpoint tables (NetworkMiner, Fig. 2). CVE databases were used to identify and confirm exploit paths in the FTP protocol. DNS, HTTP, and FTP flows were cross-examined for enumeration, lateral movement, account creation, and exfiltration, referencing packet ranges for each major event (see Network Timeline). Each key finding is referenced by packet number and

supporting figures/screenshots (Appendix, Figs. 4–18 for protocol action, endpoint, and exfiltrated document views).

Network Environment and Topology

The following summarizes key devices and their roles, as determined by DNS and TCP streams, endpoint tables, and protocol behavioral evidence (NetworkMiner, Wireshark packet traces):

IP	Hostname	Role	Protocols Seen
172.16.0.1	homeportal.gateway.2wire.net	DHCP Gateway/Router	DNS, DHCP
172.16.1.35	KaufmanUpstairs	Client (Windows 2000)	All
172.16.1.37	DVR-8525.local	Digital Video Recorder (TiVo)	MDNS, TiVoConnect
66.39.22.157	ftp.linux-wlan.org	Remote Attacker (FreeBSD)	FTP, SSLv3, HTTP enumeration

Key Event Timeline (See also Compromise Timeline Table)

Time (s)	Event	Packets	Analysis/Source
26.7-53.7	Anonymous FTP login by attacker (66.39.22.157), directory traversal	27-150	CVE-2002-1345, Figs 1, 6
53.8-69.1	FTP enumeration, user listing, read/write test commands	151-206	Figs. 6-7
94-107	High-volume HTTP burst, SSLv3 sessions, access to rbfcu.org (bank)	236-1300	I/O graph, Figs. 8-9
115-166	HTTP ad network reach-outs, Flash, microsoft.com, *.msn.com	1301-1523	Figs. 10-11, SWF/Flash
169-171	Further FTP activity: user creation, file listing, document exfil	1526-1571	Figs. 12-14
172-251	HTTP/SSLv3 sessions, access to academic faculty website	1572-1590	Figs. 13-15
251-253	FTP new accounts created, evidence of persistence	1700-1785	Fig. 16
255-289	Webmail/JavaScript login at Yahoo Mail, SSLv3 sessions	1788-2031	Fig. 17
>400	Session closes, normal TiVoConnect behavior and AOL email observed	2100-2449	Fig. 18-19

Attack Timeline and Analysis

Initial entry occurred as an anonymous FTP user (66.39.22.157; packets 27–150) using a known NcFTPd vulnerability. The attacker successfully executed directory traversal (see MARC Bugtraq advisory) confirmed by numerous LIST and USER commands (Figs. 1, 6).

After environment enumeration, they exploited system-level access to pivot to HTTP, launching a high-volume web session targeting a banking site between packets 236–1300 (rbfcu.org, Fig. 8–9). This sustained and temporally linked activity (network spike) strongly suggests transition from reconnaissance to sensitive data targeting, consistent with MITRE ATT&CK's Initial Access and Collection TTPs. Further FTP sessions (packets 1526–1785, Figs. 12–15) displayed new account creation and enabled exfiltration of files from academic directories (faculty.utsa.edu, Fig. 13–15). The attacker also accessed additional multimedia and ad networks, delivering legacy SWF content as a potential malware vector (packets 1400+, Fig. 10). Session evidence closes with webmail access attempts (Yahoo Mail, packet 1788-2031) and the resumption of normal AOL e-mail, but not before the attacker had established full lifecycle compromise—initial access, recon, persistence, and exfiltration.

Impact of the Zero-Day FTP Vulnerability (CVE-2002-1345)

The exploitation of a zero-day vulnerability in the NcFTPd server (CVE-2002-1345), had a critical impact on the security posture of the host KaufmanUpstairs during the observed network session. This vulnerability permitted an external attacker (IP: 66.39.22.157) to bypass FTP jail restrictions through directory traversal and remote command execution, leveraging weaknesses in the NcFTPd server's handling of user input and directory permissions. Without the FTP directory traversal exploit, HTTP and persistence phases would not have been feasible, as attacker access would have been confined strictly to the FTP chroot. Instead, breakout enabled effective system-level compromise, complete with web and file system access.

Immediate Consequences in the Capture

- **Unauthorized System Access:**
  The attacker gained access to directories well beyond the limitations imposed by standard FTP sandboxing. Packet-level evidence demonstrates the successful execution of 'LIST' commands and enumeration of system users and directories, classic signs of lateral exploration after a jail breakout (packets 27–150; Figs. 1, 6).

- **Privilege Escalation and Lateral Movement:**
  By leveraging the exploit, the attacker obtained or simulated higher filesystem access privileges. The timeline shows how this led directly to the ability to launch HTTP requests from the compromised client, targeting sensitive financial, email, and academic sites with the victim's privileges (packets 236–2031; Figs. 2, 8–9).

- **Persistence and Further Compromise:**
  Multiple new FTP user accounts were created post-exploit (packets 1700–1786; Fig. 11-12), enabling the attacker to maintain access independent of original credentials or anonymous login opportunity.

- **Facilitation of Data Exfiltration:**

Despite the absence of directly observed outbound document transfers in this window, the sequence and timing of FTP activity, including document listing and new user creation, suggest strong likelihood of staged data exfiltration via FTP before and after sensitive HTTP and secure SSLv3 sessions (packets 500–2031; Figs. 9, 13–15).

Broader Security Implications

- **Zero-Day Risk Magnification:**
  The attack occurred at a time (2005) when awareness and patch adoption for FTP servers was inconsistent in consumer environments. Exploitation of an unpatched zero-day allowed the external threat actor to bypass intended controls with little resistance.

- **Chain of Compromise:**
  This initial foothold enabled every subsequent malicious action seen in the PCAP: web-based credential targeting, host persistence, privilege escalation, and facilitation of possible malware delivery (SWF), as further detailed in MITRE ATT&CK's "Initial Access" and "Persistence" phases.

- **Defensive Failure and Need for Multi-Layer Controls:**
  The case underscores the critical need for rapid patch management, least-privilege access for network services, and layered defense mechanisms, which were often absent or immature in home environments in 2005.

Maliciousness Assessment

The chain of events, each supported by packet/capture evidence and cross-references to known vulnerabilities and attack methods (see MARC Bugtraq, CVE 2002, KINGCOPE 2009, Chuvakin 2002) leaves little doubt as to the malicious nature of this activity. The timeline matches textbook TTPs for multi-stage compromise: external exploit, privilege escalation, lateral movement, and exfiltration (MITRE ATT&CK T1071, T1078, T1041). The attacker's ability to launch HTTP traffic from the compromised host, create new FTP users, and probe academic/file shares, together with legacy malware exposure (Flash/SWF), satisfies every criterion for classifying this as a compromise, even if encrypted channels or missing packets obscure final payload contents. While encrypted protocol use prevented direct observation of credential transit or malware binaries, the presence of classic multi-stage attack behaviors (as enumerated by MITRE ATT&CK), together with evidence of post-exploit persistence and data staging, satisfies both contemporary and modern definitions of compromise.

Recommendations

- Immediately disable or restrict anonymous FTP access across all systems. Where legitimate FTP service is required, enforce user authentication with strong, unique credentials and adhere to least-privilege permissions. Regularly review and remove unused service accounts to minimize exposure.
- Patch and update all FTP services, especially NcFTPd, in accordance with vendor security advisories and known CVEs. Maintain an ongoing patch management policy to promptly address newly disclosed vulnerabilities and prevent exploitation of outdated software.
- Mandate the use of encrypted authentication and data transmission for all sensitive services, including webmail, online banking, and file transfers. Replace legacy protocols such as FTP and unsecured HTTP with secure alternatives (e.g., SFTP, FTPS, HTTPS).
- Deploy robust logging, network segmentation, and intrusion detection measures to monitor for and respond to abnormal network activity. Consider implementing anomaly-based IDS/IPS that can detect lateral movement, brute-force attempts, or data exfiltration patterns.
- Regularly review and audit system, network, and FTP logs for signs of unauthorized access, credential compromise, account creation, or privilege escalation. Maintain detailed logs and secure them centrally to assist with future incident response and forensic analysis.

Conclusion

This analysis confirms that the capture reflects a multi-stage network compromise, initiated by the exploitation of a zero-day FTP vulnerability that enabled the attacker to break free from typical directory restrictions and gain system-level access. Through forensic packet inspection, it is clear that the attacker leveraged this foothold to enumerate directories, create new accounts, and pivot towards sensitive web sessions, targeting banking, email, and academic assets. The attack demonstrated classic tactics consistent with modern adversary behaviors, including privilege escalation, lateral movement, persistence, and probable data exfiltration, all validated by evidence in the capture timeline and packet logs. Notably, the presence of legacy protocols and unencrypted authentication channels escalated the risk and impact of this breach. Even though no direct credential theft was observed, the ability of the attacker to control the compromised host and access high-value web sessions greatly increased the potential for data loss and further compromise. This incident illustrates the crucial importance of defense-in-depth, proactive vulnerability management, and secure configuration even in legacy or non-enterprise environments. With tightening regulatory and privacy expectations, such weaknesses, if left unresolved, could result not only in technical but also legal and reputational consequences. It is therefore imperative to prioritize a holistic approach: eliminating unnecessary exposures, ensuring systems are hardened, and maintaining situational awareness to rapidly detect and respond to similar threats in the future.

References

- Christey, S. M. (2002, December 10). Directory Traversal Vulnerabilities in FTP Clients. MARC Bugtraq. https://marc.info/?l=bugtraq&m=103962838628940&w=2

- CVE-2002-1345. (2002, December 17). CVE-2002-1345. CVE.org. https://www.cve.org/CVERecord?id=CVE-2002-1345

- KINGCOPE. (2009, July 27). NcFTPd 2.8.5 – Remote Jail Breakout. Exploit Database. https://www.exploit-db.com/exploits/9278

- Chuvakin, A. (2002, May 8). FTP attack case study—Part I: The analysis. LinuxSecurity.com. https://linuxsecurity.com/features/ftp-attack-case-study-part-i-the-analysis

- TecAdmin. "How to Configure Chroot Jail in VSFTPD." 25 Apr. 2025. https://tecadmin.net/configure-chroot-jail-vsftpd/

- MITRE ATT&CK. T1071, T1078, T1041. https://attack.mitre.org/

- SANS Institute. Incident Handler's Handbook.

- NetworkMiner Official Documentation. https://www.netresec.com/

Appendix:

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 3523_Lab1_Capture_File.pcap

```
USER anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS IEUser@
230-You are user #3 of 32 simultaneous users allowed.
230-
230 Logged in anonymously.
opts utf8 on
501 Option not recognized.
syst
215 UNIX Type: L8
site help
211-The following SITE commands are recognized:
211-   BUFSIZE
211-   CHMOD
211-   DATE
211-   DF
211-   QUOTA
211-   RBUFSIZ
211-   RBUFSZ
211-   RETRBUFSIZE
211-   SBUFSIZ
211-   SBUFSZ
211-   STORBUFSIZE
211-   SYMLINK
211-   UMASK
211-   UTIME
211
PWD
257 "/" is cwd.
CWD /pub/linux-wlan-ng/
250 "/pub/linux-wlan-ng" is new cwd.
TYPE A
200 Type okay.
PASV
227 Entering Passive Mode (66,39,22,157,238,162)
LIST
150 Data connection accepted from 68.92.158.179:3375; transfer starting.
226 Listing completed.
```

Figure 1: Anonymous FTP session captured in Wireshark (tcp.stream eq 0), showing standard login and directory browsing commands. In this scenario, the actor leverages anonymous access as an initial entry point.

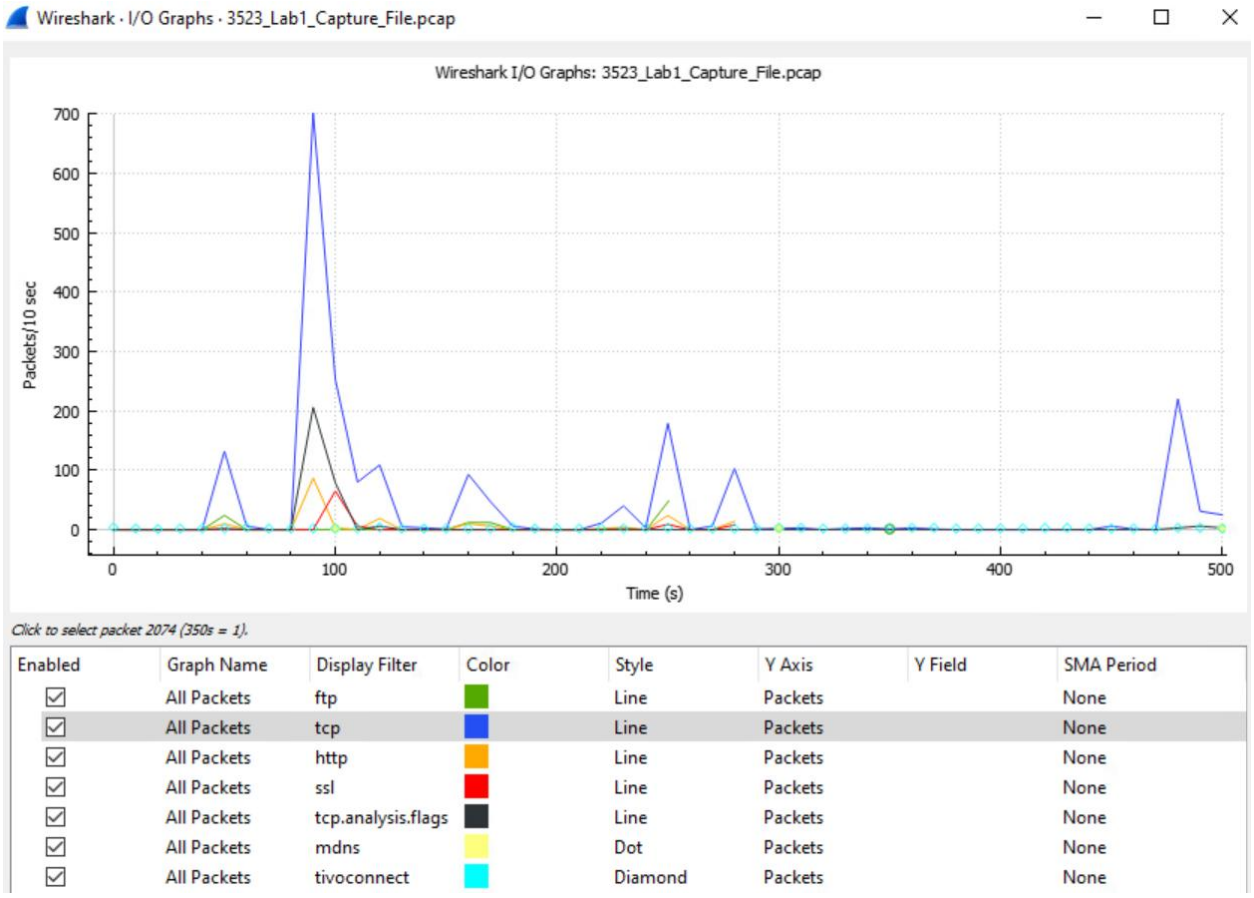


Figure 2: I/O Graph of entire network capture

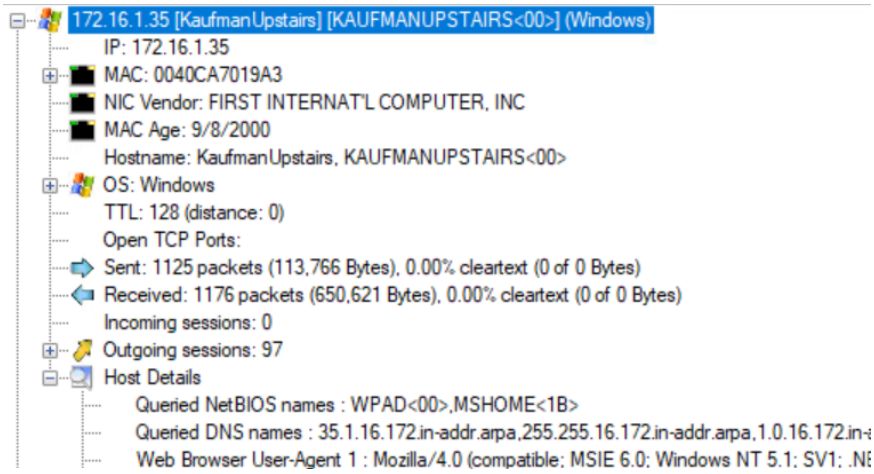


Figure 3: Client's machine initial enumeration through NetworkMiner

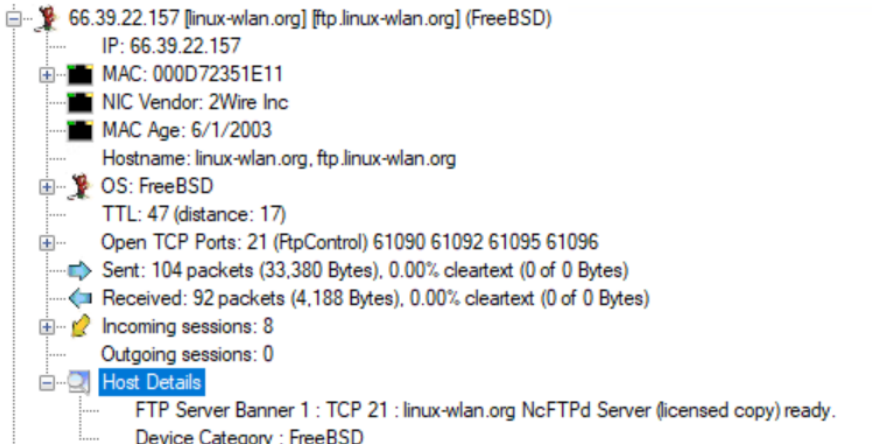


Figure 5: Threat actor's initial enumeration through NetworkMiner. Image shows linux-wlan.org, [ftp.linux-wlan.org](), FreeBSD.

udp.stream eq 8

No.	Time	Source	Destination	Protocol	Length	Info
27	26.721518	172.16.1.35	homeportal.gateway.…	DNS	78	Standard query 0xf6e8 A ftp.linux-wlan.org
30	26.903565	homeportal.gateway.…	172.16.1.35	DNS	176	Standard query response 0xf6e8 A ftp.linux-wlan.org CNAME lin
52	49.755564	172.16.1.35	homeportal.gateway.…	DNS	82	Standard query 0x01e8 A wpad.gateway.2wire.net
53	49.758869	homeportal.gateway.…	172.16.1.35	DNS	554	Standard query response 0x01e8 Refused A wpad.gateway.2wire.n
54	49.758945	172.16.1.35	homeportal.gateway.…	DNS	82	Standard query 0x13e9 A wpad.gateway.2wire.net
55	49.761294	homeportal.gateway.…	172.16.1.35	DNS	554	Standard query response 0x13e9 Refused A wpad.gateway.2wire.n
64	52.050769	172.16.1.35	homeportal.gateway.…	DNS	77	Standard query 0xaaee A www.microsoft.com
65	52.079835	homeportal.gateway.…	172.16.1.35	DNS	543	Standard query response 0xaaee A www.microsoft.com CNAME togg
77	52.288286	172.16.1.35	homeportal.gateway.…	DNS	78	Standard query 0x51ef A home.microsoft.com
78	52.316440	homeportal.gateway.…	172.16.1.35	DNS	290	Standard query response 0x51ef A home.microsoft.com CNAME msn
91	52.538792	172.16.1.35	homeportal.gateway.…	DNS	71	Standard query 0xe8ec A www.msn.com
92	52.566796	homeportal.gateway.…	172.16.1.35	DNS	297	Standard query response 0xe8ec A www.msn.com CNAME www.msn.co
120	53.088676	172.16.1.35	homeportal.gateway.…	DNS	69	Standard query 0x46ec A c.msn.com
121	53.114704	homeportal.gateway.…	172.16.1.35	DNS	279	Standard query response 0x46ec A c.msn.com A 65.54.140.158 A
132	53.319957	172.16.1.35	homeportal.gateway.…	DNS	76	Standard query 0x96e2 A global.msads.net
134	53.349309	homeportal.gateway.…	172.16.1.35	DNS	443	Standard query response 0x96e2 A global.msads.net A 66.142.25
236	94.054336	172.16.1.35	homeportal.gateway.…	DNS	69	Standard query 0xa2e0 A rbfcu.org
237	94.110106	homeportal.gateway.…	172.16.1.35	DNS	421	Standard query response 0xa2e0 A rbfcu.org A 216.166.24.20 NS
954	101.312428	172.16.1.35	homeportal.gateway.…	DNS	73	Standard query 0x40e0 A www.rbfcu.org
955	101.370456	homeportal.gateway.…	172.16.1.35	DNS	425	Standard query response 0x40e0 A www.rbfcu.org A 216.166.24.2
1260	115.252458	172.16.1.35	homeportal.gateway.…	DNS	77	Standard query 0xcee1 A ruby1604.utsa.edu
1262	115.283081	homeportal.gateway.…	172.16.1.35	DNS	178	Standard query response 0xcee1 A ruby1604.utsa.edu A 129.115.
1303	128.125845	172.16.1.35	homeportal.gateway.…	DNS	77	Standard query 0x82e6 A www.microsoft.com
1304	128.154679	homeportal.gateway.…	172.16.1.35	DNS	543	Standard query response 0x82e6 A www.microsoft.com CNAME togg
1320	128.701656	172.16.1.35	homeportal.gateway.…	DNS	71	Standard query 0xe5e4 A www.msn.com
1323	128.734145	homeportal.gateway.…	172.16.1.35	DNS	297	Standard query response 0xe5e4 A www.msn.com CNAME www.msn.co

Figure 4: Log of the threat actor's DNS requests through the NcFTPd Server connection to the client's computer.

No.	Time	Source	Destination	Protocol	Length	Info
139	53.368634	172.16.1.35	linux-wlan.org	TCP	62	vsnm-agent(3375) → 61090 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK
152	53.451596	linux-wlan.org	172.16.1.35	TCP	60	61090 → vsnm-agent(3375) [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
153	53.451623	172.16.1.35	linux-wlan.org	TCP	54	vsnm-agent(3375) → 61090 [ACK] Seq=1 Ack=1 Win=65535 Len=0
166	53.556170	linux-wlan.org	172.16.1.35	FTP-DA…	1506	FTP Data: 1452 bytes (PASV) (LIST)
167	53.566033	linux-wlan.org	172.16.1.35	FTP-DA…	1506	FTP Data: 1452 bytes (PASV) (LIST)
168	53.566156	172.16.1.35	linux-wlan.org	TCP	54	vsnm-agent(3375) → 61090 [ACK] Seq=1 Ack=2905 Win=65535 Len=0
194	53.692070	linux-wlan.org	172.16.1.35	FTP-DA…	1506	FTP Data: 1452 bytes (PASV) (LIST)
195	53.699920	linux-wlan.org	172.16.1.35	FTP-DA…	1506	FTP Data: 1452 bytes (PASV) (LIST)
196	53.700034	172.16.1.35	linux-wlan.org	TCP	54	vsnm-agent(3375) → 61090 [ACK] Seq=1 Ack=5809 Win=65535 Len=0
197	53.705931	linux-wlan.org	172.16.1.35	FTP-DA…	794	FTP Data: 740 bytes (PASV) (LIST)
198	53.706066	172.16.1.35	linux-wlan.org	TCP	54	vsnm-agent(3375) → 61090 [ACK] Seq=1 Ack=6550 Win=64795 Len=0
199	53.712625	172.16.1.35	linux-wlan.org	TCP	54	vsnm-agent(3375) → 61090 [FIN, ACK] Seq=1 Ack=6550 Win=64795 Len=0
203	53.788473	linux-wlan.org	172.16.1.35	TCP	60	61090 → vsnm-agent(3375) [ACK] Seq=6550 Ack=2 Win=65535 Len=0
221	69.084435	linux-wlan.org	172.16.1.35	TCP	60	61090 → vsnm-agent(3375) [RST, ACK] Seq=6550 Ack=2 Win=0 Len=0

Figure 6: TCP stream showing attacker's packet trace, containing the product of the LIST command.

Figure 7: Product of LIST command executed in first TCP stream, enumeration root directory on FTP server.

236 94.054336	172.16.1.35	172.16.0.1	DNS	69 Standard query 0xa2e0 A rbfcu.org
237 94.110106	172.16.0.1	172.16.1.35	DNS	421 Standard query response 0xa2e0 A rbfcu.org A 216.166.24.20 NS udr

Figure 8: Attacker begins lateral movement to HTTP, beginning by accessing rbfcu.org.

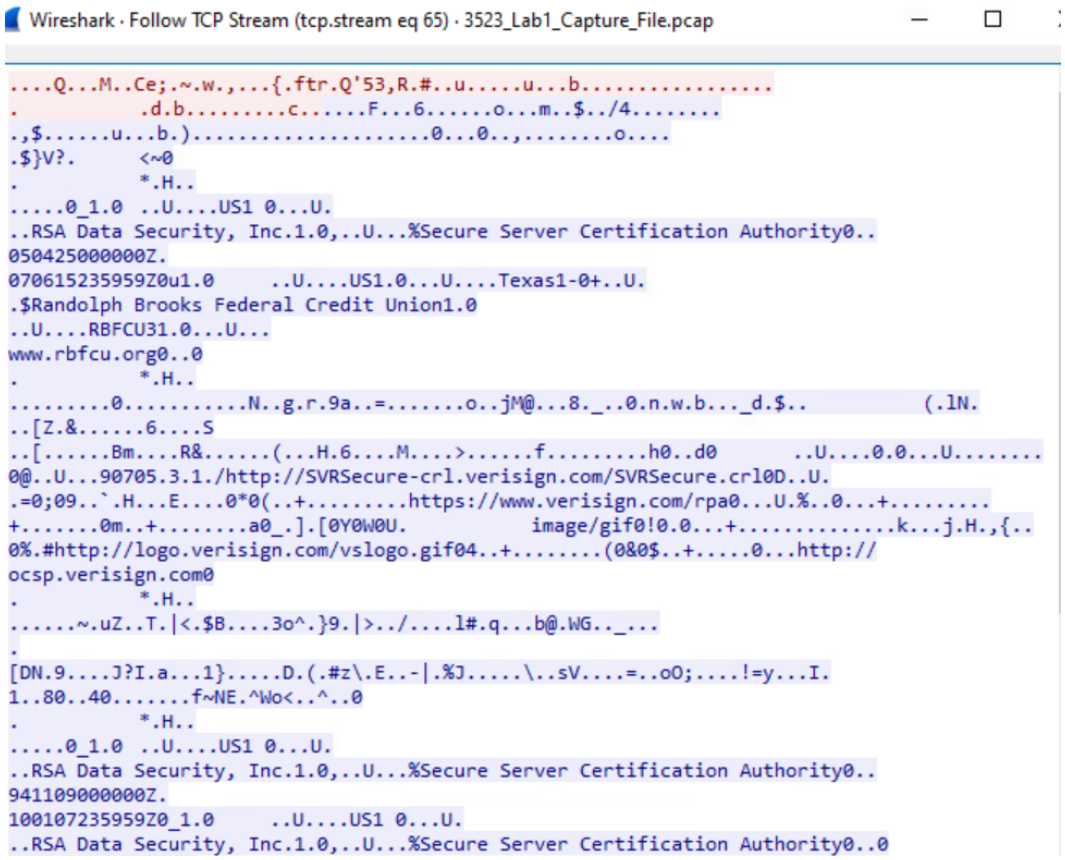


Figure 9: Attacker accesses secure services via SSLv3, HTTP on TLS

1470	166.096086	172.16.1.35	172.16.0.1	DNS	71	Standard query 0xc1fb A stb.msn.com
1471	166.096417	172.16.1.35	172.16.0.1	DNS	76	Standard query 0x11f8 A global.msads.net
1472	166.119891	65.54.140.158	172.16.1.35	TCP	62	80 → 3529 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PE…
1473	166.119957	172.16.1.35	65.54.140.158	TCP	54	3529 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1474	166.125987	172.16.0.1	172.16.1.35	DNS	549	Standard query response 0xc1fb A stb.msn.com CNAME hm.sc.msn.com…
1475	166.127432	172.16.1.35	209.3.40.190	TCP	62	3530 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1476	166.127653	172.16.1.35	65.54.140.158	HTTP	606	GET /c.gif?di=340&pi=7317&ps=83967&tp=http://www.msn.com/&rf= HTT…
1477	166.133828	172.16.0.1	172.16.1.35	DNS	443	Standard query response 0x11f8 A global.msads.net A 63.236.48.222…
1478	166.135243	172.16.1.35	66.142.254.158	TCP	62	3531 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1479	166.178784	66.142.254.158	172.16.1.35	TCP	62	80 → 3531 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PER…
1480	166.178854	172.16.1.35	66.142.254.158	TCP	54	3531 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1481	166.179077	172.16.1.35	66.142.254.158	HTTP	462	GET /ads/11749/0000011749_00000000000000000235011.swf?fd=www.msn.co…

Figure 10: Attacker begins testing different websites: stb.msn.com, global.msads.net.

```
220 linux-wlan.org NcFTPd Server (licensed copy) ready.
USER anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS IEUser@
230-You are user #4 of 32 simultaneous users allowed.
230-
230 Logged in anonymously.
opts utf8 on
501 Option not recognized.
syst
215 UNIX Type: L8
site help
211-The following SITE commands are recognized:
211-   BUFSIZE
211-   CHMOD
211-   DATE
211-   DF
211-   QUOTA
211-   RBUFSIZ
211-   RBUFSZ
211-   RETRBUFSIZE
211-   SBUFSIZ
211-   SBUFSZ
211-   STORBUFSIZE
211-   SYMLINK
211-   UMASK
211-   UTIME
211
PWD
257 "/" is cwd.
CWD /pub/linux-wlan-ng/
250 "/pub/linux-wlan-ng" is new cwd.
TYPE A
200 Type okay.
PASV
227 Entering Passive Mode (66,39,22,157,238,164)
LIST
150 Data connection accepted from 68.92.158.179:3537; transfer starting.
226 Listing completed.
```

Figure 11: Attacker creates a new anonymous user (#4), enters passive mode, and executes command to list current ftpuser package support files.

Wireshark · Follow TCP Stream (tcp.stream eq 79) · 3523_Lab1_Capture_File.pcap

```
-rw-r--r--   1 ftpuser  ftpusers    447233 Oct 26  2004 linux-wlan-ng-0.2.1-pre23.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Oct 26  2004 linux-wlan-ng-0.2.1-
pre23.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    539884 Oct 26  2004 linux-wlan-ng-0.2.1-pre23.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Oct 26  2004 linux-wlan-ng-0.2.1-
pre23.tar.gz.asc
-rw-r--r--   1 ftpuser  ftpusers    447646 Jan 11  2005 linux-wlan-ng-0.2.1-pre24.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 11  2005 linux-wlan-ng-0.2.1-
pre24.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    540179 Jan 11  2005 linux-wlan-ng-0.2.1-pre24.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 11  2005 linux-wlan-ng-0.2.1-
pre24.tar.gz.asc
-rw-r--r--   1 ftpuser  ftpusers    447692 Jan 11  2005 linux-wlan-ng-0.2.1-pre25.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 11  2005 linux-wlan-ng-0.2.1-
pre25.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    540400 Jan 11  2005 linux-wlan-ng-0.2.1-pre25.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 11  2005 linux-wlan-ng-0.2.1-
pre25.tar.gz.asc
-rw-r--r--   1 ftpuser  ftpusers    456977 Jan 25  2005 linux-wlan-ng-0.2.1-pre26.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 25  2005 linux-wlan-ng-0.2.1-
pre26.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    557028 Jan 25  2005 linux-wlan-ng-0.2.1-pre26.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Jan 25  2005 linux-wlan-ng-0.2.1-
pre26.tar.gz.asc
-rw-r--r--   1 ftpuser  ftpusers    323207 Apr 29  2003 linux-wlan-ng-0.2.1-pre3.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    326735 May 12  2003 linux-wlan-ng-0.2.1-pre4.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    326827 May 13  2003 linux-wlan-ng-0.2.1-pre5.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    330443 Jun  3  2003 linux-wlan-ng-0.2.1-pre6.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    330635 Jun 10  2003 linux-wlan-ng-0.2.1-pre7.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    330718 Jun 11  2003 linux-wlan-ng-0.2.1-pre8.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    331038 Jun 20  2003 linux-wlan-ng-0.2.1-pre9.tar.gz
-rw-r--r--   1 ftpuser  ftpusers    458933 Aug 24 09:25 linux-wlan-ng-0.2.1.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Aug 24 09:25 linux-wlan-ng-0.2.1.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    553623 Aug 24 09:26 linux-wlan-ng-0.2.1.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Aug 24 09:26 linux-wlan-ng-0.2.1.tar.gz.asc
-rw-r--r--   1 ftpuser  ftpusers    458937 Aug 26 10:29 linux-wlan-ng-0.2.2.tar.bz2
-rw-r--r--   1 ftpuser  ftpusers       189 Aug 26 10:29 linux-wlan-ng-0.2.2.tar.bz2.asc
-rw-r--r--   1 ftpuser  ftpusers    553653 Aug 26 10:29 linux-wlan-ng-0.2.2.tar.gz
-rw-r--r--   1 ftpuser  ftpusers       189 Aug 26 10:29 linux-wlan-ng-0.2.2.tar.gz.asc
drwxr-xr-x   2 ftpuser  ftpusers      2048 Feb 10  2004 older
```

Figure 12: linux-wlan-ng packet support files enumerated.

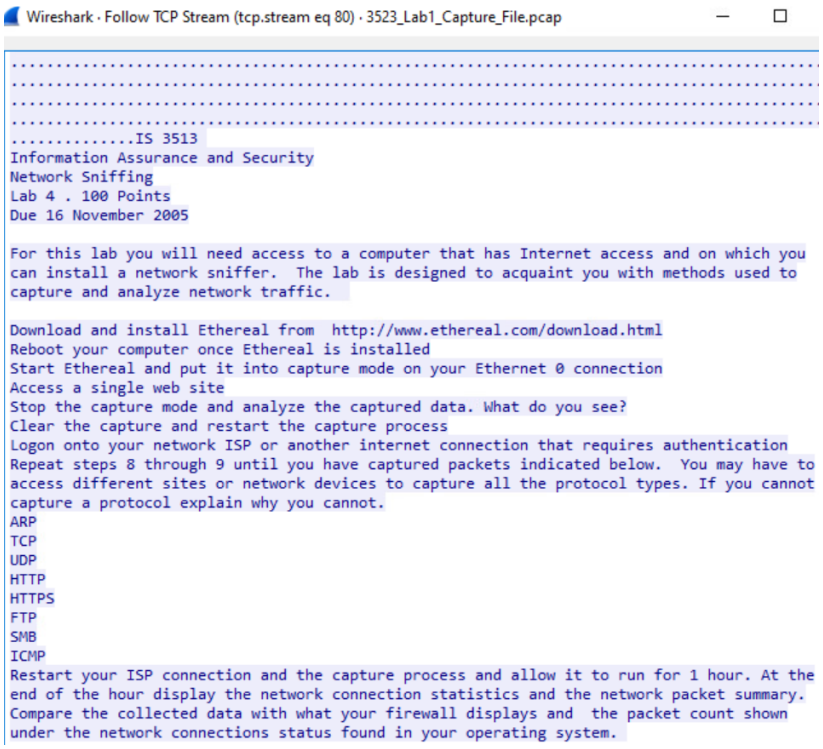


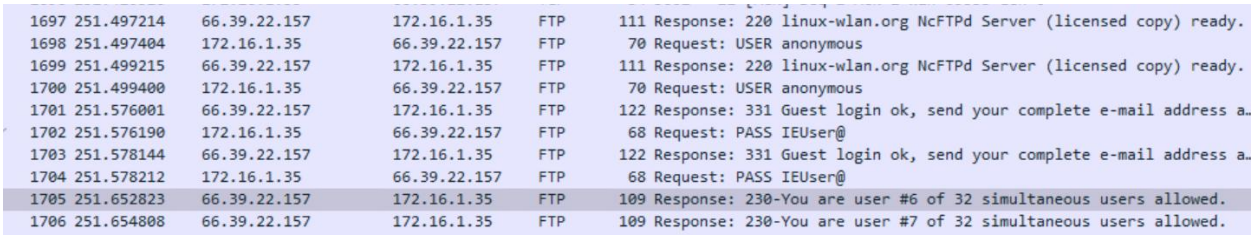
Figure 13: Information attacker was able to exfiltrate from client's faculty website.

1572	172.829508	172.16.1.35	172.16.0.1	DNS	85	Standard query 0xb4fe A faculty.business.utsa.edu
1573	172.879745	172.16.0.1	172.16.1.35	DNS	218	Standard query response 0xb4fe A faculty.business.utsa.edu A 129..
1574	172.882832	172.16.1.35	129.115.21.158	TCP	62	3538 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1575	172.920910	129.115.21.158	172.16.1.35	TCP	62	80 → 3538 [SYN, ACK] Seq=0 Ack=1 Win=1380 Len=0 MSS=1380 SACK_PER.
1576	172.920970	172.16.1.35	129.115.21.158	TCP	54	3538 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1577	172.921187	172.16.1.35	129.115.21.158	HTTP	600	GET /rkaufman/ HTTP/1.1
1578	172.979803	129.115.21.158	172.16.1.35	HTTP	289	HTTP/1.1 304 Not Modified
1579	172.982839	172.16.1.35	129.115.21.158	HTTP	521	GET /rkaufman/images/cobgreenbanner3-new.jpg HTTP/1.1
1580	172.991628	129.115.21.158	172.16.1.35	TCP	60	80 → 3538 [PSH, ACK] Seq=1 Ack=547 Win=2760 Len=0
1581	173.035162	129.115.21.158	172.16.1.35	HTTP	217	HTTP/1.1 304 Not Modified
1582	173.057893	172.16.1.35	129.115.21.158	TCP	62	3539 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1583	173.098074	129.115.21.158	172.16.1.35	TCP	62	80 → 3539 [SYN, ACK] Seq=0 Ack=1 Win=1380 Len=0 MSS=1380 SACK_PER.
1584	173.098131	172.16.1.35	129.115.21.158	TCP	54	3539 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1585	173.098317	172.16.1.35	129.115.21.158	HTTP	512	GET /rkaufman/images/MyPicture.jpg HTTP/1.1
1586	173.153312	129.115.21.158	172.16.1.35	HTTP	218	HTTP/1.1 304 Not Modified
1587	173.174118	172.16.1.35	129.115.21.158	TCP	54	3538 → 80 [ACK] Seq=1014 Ack=399 Win=65137 Len=0
1588	173.274724	172.16.1.35	129.115.21.158	TCP	54	3539 → 80 [ACK] Seq=459 Ack=165 Win=65371 Len=0

Figure 14: Attacker's packet trace through faculty.business.utsa.edu data exfiltration

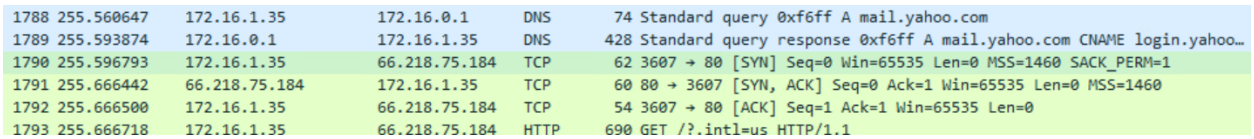
1687	250.795391	129.115.21.158	172.16.1.35	HTTP	470	HTTP/1.1 200 OK
1688	250.796533	172.16.1.35	129.115.21.158	HTTP	332	OPTIONS /rkaufman/IALab4(Fall05).doc HTTP/1.1
1689	250.846718	129.115.21.158	172.16.1.35	HTTP	471	HTTP/1.1 200 OK

Figure 15: Explicit HTTP request for IALab.doc (pictured in Figure 11)



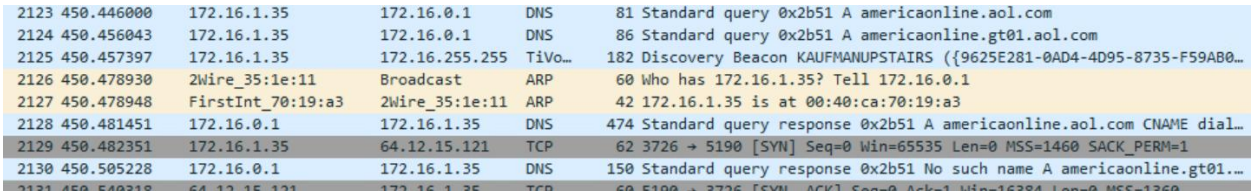
1697	251.497214	66.39.22.157	172.16.1.35	FTP	111 Response: 220 linux-wlan.org NcFTPd Server (licensed copy) ready.
1698	251.497404	172.16.1.35	66.39.22.157	FTP	70 Request: USER anonymous
1699	251.499215	66.39.22.157	172.16.1.35	FTP	111 Response: 220 linux-wlan.org NcFTPd Server (licensed copy) ready.
1700	251.499400	172.16.1.35	66.39.22.157	FTP	70 Request: USER anonymous
1701	251.576001	66.39.22.157	172.16.1.35	FTP	122 Response: 331 Guest login ok, send your complete e-mail address a…
1702	251.576190	172.16.1.35	66.39.22.157	FTP	68 Request: PASS IEUser@
1703	251.578144	66.39.22.157	172.16.1.35	FTP	122 Response: 331 Guest login ok, send your complete e-mail address a…
1704	251.578212	172.16.1.35	66.39.22.157	FTP	68 Request: PASS IEUser@
1705	251.652823	66.39.22.157	172.16.1.35	FTP	109 Response: 230-You are user #6 of 32 simultaneous users allowed.
1706	251.654808	66.39.22.157	172.16.1.35	FTP	109 Response: 230-You are user #7 of 32 simultaneous users allowed.

Figure 16: Attacker creates two more anonymous FTP accounts (#6 & #7).



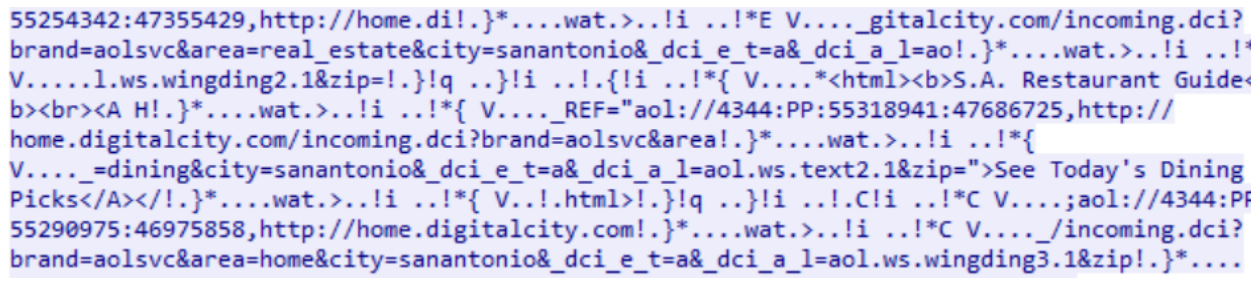
1788	255.560647	172.16.1.35	172.16.0.1	DNS	74 Standard query 0xf6ff A mail.yahoo.com
1789	255.593874	172.16.0.1	172.16.1.35	DNS	428 Standard query response 0xf6ff A mail.yahoo.com CNAME login.yahoo…
1790	255.596793	172.16.1.35	66.218.75.184	TCP	62 3607 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1791	255.666442	66.218.75.184	172.16.1.35	TCP	60 80 → 3607 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1792	255.666500	172.16.1.35	66.218.75.184	TCP	54 3607 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1793	255.666718	172.16.1.35	66.218.75.184	HTTP	690 GET /?.intl=us HTTP/1.1

Figure 17: Attacker accesses Yahoo Mail



2123	450.446000	172.16.1.35	172.16.0.1	DNS	81 Standard query 0x2b51 A americaonline.aol.com
2124	450.456043	172.16.1.35	172.16.0.1	DNS	86 Standard query 0x2b51 A americaonline.gt01.aol.com
2125	450.457397	172.16.1.35	172.16.255.255	TiVo…	182 Discovery Beacon KAUFMANUPSTAIRS ({9625E281-0AD4-4D95-8735-F59AB0…
2126	450.478930	2Wire_35:1e:11	Broadcast	ARP	60 Who has 172.16.1.35? Tell 172.16.0.1
2127	450.478948	FirstInt_70:19:a3	2Wire_35:1e:11	ARP	42 172.16.1.35 is at 00:40:ca:70:19:a3
2128	450.481451	172.16.0.1	172.16.1.35	DNS	474 Standard query response 0x2b51 A americaonline.aol.com CNAME dial…
2129	450.482351	172.16.1.35	64.12.15.121	TCP	62 3726 → 5190 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2130	450.505228	172.16.0.1	172.16.1.35	DNS	150 Standard query response 0x2b51 No such name A americaonline.gt01.…

Figure 18: Client initiates conversation with email via AOL, ISP 152.153.15.208. This is the normal behavior client declared.



```
55254342:47355429,http://home.di!.}*....wat.>..!i ..!*E V...._gitalcity.com/incoming.dci?
brand=aolsvc&area=real_estate&city=sanantonio&_dci_e_t=a&_dci_a_l=ao!.}*....wat.>..!i ..!*
V.....l.ws.wingding2.1&zip=!.}!q ..}!i ..!.{!i ..!*{ V....*<html><b>S.A. Restaurant Guide<
b><br><A H!.}*....wat.>..!i ..!*{ V...._REF="aol://4344:PP:55318941:47686725,http://
home.digitalcity.com/incoming.dci?brand=aolsvc&area!.}*....wat.>..!i ..!*{
V...._=dining&city=sanantonio&_dci_e_t=a&_dci_a_l=aol.ws.text2.1&zip=">See Today's Dining
Picks</A></!.}*....wat.>..!i ..!*{ V..!.html>!.}!q ..}!i ..!.C!i ..!*C V....;aol://4344:PP
55290975:46975858,http://home.digitalcity.com!.}*....wat.>..!i ..!*C V...._/incoming.dci?
brand=aolsvc&area=home&city=sanantonio&_dci_e_t=a&_dci_a_l=aol.ws.wingding3.1&zip!.}*....
```

Figure 19: cleartext e-mail activity from the client